

SVEUČILIŠTE U ZAGREBU  
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA  
EKONOMSKI FAKULTET

SVEUČILIŠTE J.J. STROSSMAYERA U OSIJEKU  
ELEKTROTEHNIČKI FAKULTET

SVEUČILIŠTE U SPLITU  
FAKULTET ELEKTROTEHNIKE, STROJARSTVA I BRODOGRADNJE

# Pogled u budućnost

---

Projekt suradnje s  
Hrvatskom agencijom za poštu i elektroničke komunikacije

*Izvješće 2014*

*Mjerenje brzine pristupa u 4G LTE mreža, prijetnje korisnicima telekomunikacijskih usluga, kalkulator za procjenu rizika povrede privatnosti korisnika, regulatorni aspekti budućih mreža, privatnost i uključivost usluga i njihova kvaliteta*



Zagreb, 2014.

## Sadržaj

<b>1. Mjerenje brzine pristupa u 4G LTE mreži .....</b>	<b>6</b>
1.1. Sažetak .....	6
1.2. Uvod.....	7
1.3. Obilježja LTE mreža .....	8
1.4. Mjerni alati .....	11
1.5. Rezultati .....	12
1.6. Zaključak.....	16
1.7. Literatura .....	17
<b>2. Prijetnje korisnicima telekomunikacijskih usluga i kalkulator za procjenu rizika povrede privatnosti korisnika .....</b>	<b>19</b>
1.1. Uvod.....	19
1.2. Najčešće prijetnje .....	20
1.3. Savjeti za izbjegavanje internetskih prijevara.....	27
1.4. Svojevoljno ostavljanje podataka.....	28
1.4.1. Društvene mreže.....	28
1.4.2. <i>Loyalty</i> programi .....	28
1.4.3. <i>Online</i> download igara .....	29
1.5. Kalkulator rizika.....	29
1.6. Zaključak .....	32
1.7. Literatura .....	33
<b>3. Evaluacija kalkulatora za procjenu rizika povrede privatnosti korisnika.....</b>	<b>34</b>
3.1. Uvod.....	34
3.2. Srodna istraživanja .....	35
3.3. Kalkulator rizika.....	38
3.4. Evaluacija .....	41
3.5. Zaključak .....	44
3.6. Literatura .....	45
<b>4. Simulacija načina rada i usporedba značajki sustava DVB-T i DVB-T2.....</b>	<b>47</b>
4.1. Sažetak .....	47
4.2. Uvod.....	48

4.3.	Pregled ostalih radova .....	53
4.4.	Tehnički opis sustava DVB-T i DVB-T2.....	53
4.5.	Modeli kanala.....	56
4.6.	Rezultati simulacije .....	57
4.7.	Zaključak .....	58
4.8.	Literatura .....	59
<b>5.</b>	<b>Zaštita osobnih podataka u kontekstu pružanja usluga računarstva u oblaku prema pravu Europske unije i pravu Republike Hrvatske.....</b>	<b>61</b>
5.1.	Sažetak .....	61
5.2.	Uvod.....	62
5.3.	Istraživanje i rezultati .....	63
5.3.1.	Važeći pravno-regulatorni okvir EU-a.....	63
5.3.2.	Analiza važećeg pravnog okvira Republike Hrvatske i aktivnosti nadzornog tijela u području zaštite osobnih podataka i <i>cloud computinga</i> .....	65
5.3.3.	Ispitivanje predloženih rješenja budućeg općeg okvira EU-a za zaštitu osobnih podataka u <i>cloud</i> okruženju.....	65
5.4.	Zaključak .....	67
5.5.	Literatura .....	68
<b>6.</b>	<b>Regulatorna perspektiva buduće komunikacijske mreže i Interneta .....</b>	<b>72</b>
6.1.	Uvod.....	72
6.2.	Istraživanja u području budućih mreža .....	72
6.3.	Regulatorna perspektiva.....	74
6.3.1.	Internet stvari i komunikacija strojeva .....	74
6.3.2.	Internet usluga i računarstvo u oblaku .....	76
6.4.	Regulatorni prostor.....	77
6.5.	Zaključno razmatranje.....	80
6.6.	Literatura .....	80
<b>7.</b>	<b>Istraživanje o troškovnim metodologijama u informacijskim sustavima operatora u RH .....</b>	<b>84</b>
7.1.	Uvod.....	84
7.2.	Rezultati empirijskog istraživanja.....	85
7.3.	Zaključak .....	110
7.4.	Literatura .....	111

<b>8. Radionica „The 4rd Workshop on Regulatory Challenges in the Electronic Communications Market“ .....</b>	<b>113</b>
8.1. Popis radova .....	113
<b>9. Komunikacijski sustav stroja sa strojem u javnoj pokretnoj mreži.....</b>	<b>115</b>
9.1. Uvod .....	115
9.2. Specifičnosti M2M komunikacije u javnoj pokretnoj mreži.....	115
9.2.1. Scenarij M2M uređaj-M2M poslužitelj.....	117
9.2.2. Scenarij M2M uređaj-M2M uređaj .....	118
9.3. Promjene na tržištu M2M modula u javnoj pokretnoj mreži .....	119
9.4. Evolucija M2M platformi.....	121
9.5. Aktualni izazovi u području M2M regulacije .....	123
9.6. Literatura .....	124
<b>10. Širokopojasni pristup Internetu u ruralnim područjima.....</b>	<b>126</b>
10.1. Analiza digitalnog jaza između ruralnih i urbanih područja .....	126
10.2. Smjernice za smanjenje digitalnog jaza .....	127
10.3. Analiza čimbenika koji utječu na usvajanje širokopojasnih tehnologija i usluga te na uvođenje širokopojasnog pristupa u ruralnim područjima .....	128
10.4. Prijedlog i izrada tehno-ekonomskog modela koji se zasniva na rezultatima provedenih analiza.....	130
10.5. Izbor optimalnih širokopojasnih pristupnih rješenja za odabrane ruralne scenarije ...	131
10.6. Postupci pri tehno-ekonomskom modeliranju.....	132
10.7. Zaključna razmatranja .....	137
<b>11. Usluge za osobe sa složenim komunikacijskim potrebama - pristupačnost ICT usluga i osobe starije dobi.....</b>	<b>139</b>
11.1. Uvod .....	139
11.2. Složene komunikacijske potrebe i osobe starije dobi.....	139
11.3. Osobe starije dobi i korištenje ICT usluga .....	141
11.4. Projekti koje se bave problematikom pristupačnosti tehnologije korisnicima starije dobi.....	142
11.5. Pristupačnost web sjedišta.....	144
11.6. Smjernice i preporuke za osiguranje pristupačnosti usluga weba.....	145
11.6.1. Smjernice WCAG .....	146
11.6.2. ITU preporuka: F.790 (01/07) Telecommunications accessibility guidelines for older persons and persons with disabilities .....	150

11.6.3. Smjerice pristupačnosti prema članku 508 (Section 508 Accessibility Guidelines)	150
11.6.4. Najbolje prakse/preporuke Googlea za implementaciju pristupačnosti namijenjene Android razvijateljima.....	150
11.7. Korisnička sučelja novih generacija pokretnih uređaja i korisnici starije dobi.....	150
11.7.1. Mobilne aplikacije za starije korisnike.....	151
11.8. Alati za provjeru e-pristupačnosti sjedišta weba.....	152
11.9. Analiza pristupačnosti najposjećenijih sjedišta web katoga www.hr.....	154
11.10. Ugrađene pristupačne opcije na pokretnim uređajima i računalu.....	156
11.10.1. Pristupačne opcije na uređajima s operacijskim sustavom iOS.....	157
11.10.2. Pristupačne opcije na uređajima s operacijskim sustavom Android.....	159
11.10.3. Pristupačnost na operacijskom sustavu Windows 8.1.....	160
11.10.4. Analiza opcija pristupačnosti na primjeru zadanog sjedišta weba.....	161
11.11. Zaključak.....	163
11.12. Literatura.....	163
<b>12. Kalkulator za procjenu rizika povrede privatnosti korisnika.....</b>	<b>165</b>
12.1. Uvod.....	165
12.2. Upute za korištenje.....	166
12.3. Popis stripova.....	169
12.4. Literatura.....	172

## 1. Mjerenje brzine pristupa u 4G LTE mreži

### 1.1. Sažetak

Približno dvije trećine korisnika širom svijeta pristupaju Internetu putem pokretne mreže (engl. *mobile/cellular network*). Brzine prijenosa podataka u dolaznom (engl. *downlink*) i odlaznom (engl. *uplink*) smjeru važni su čimbenici za omogućavanje određene razine kvalitete usluge (engl. *Quality of Service, QoS*) i kvalitete iskustva (engl. *Quality of Experience, QoE*). U ovom su izvješću prikazani rezultati mjerenja brzine pristupa Internetu putem pokretne mreže koja trenutno omogućuje najveću brzinu prijenosa podataka, dugoročna evolucija pokretne mreže (engl. *Long Term Evolution, LTE*). Korištena je samo ona oprema koja je na raspolaganju običnom pretplatniku te dva alata za određivanje brzine prijenosa podataka - HAKOMetar i Speedtest. Mjerenja su provedena na nekoliko lokacija u gradu Zagrebu. Rezultati su prikazani odvojeno za radni dan i vikend. Doprinos ovog rada je dvojak: prvo će se pokazati kako se brzina prijenosa podataka mijenja tijekom radnih dana i vikenda, a zatim se vrši usporedba izmjerenih brzina prijenosa podataka s podacima koje operatori pokretnih mreža oglašavaju te se pokazuje koliko se oni međusobno razlikuju.

## 1.2. Uvod

Broj pretplatnika sa širokopojasnim pristupom Internetu putem pokretne mreže povećan je s 268 milijuna u 2007. godini na 1,9 milijarde u 2013. godini, što čini pokretne mreže nove generacije najdinamičnijim sektorom globalnog ICT (*Information and communications technology*) tržišta [1], [2]. Do kraja 2014. godine broj korisnika Interneta u svijetu će doseći gotovo 3 milijarde [3], od čega će dvije trećine njih za pristup koristiti pokretne mreže. Europa ima najvišu razinu penetracije pokretnog širokopojasnog pristupa Internetu u odnosu na druge kontinente (64%), što je čak više i od njene razine fiksne širokopojasne penetracije (28%) [3]. Razlog tome je činjenica da se u fiksne pretplate ubrajaju pojedina kućanstava, dok su pokretne pretplate vezane uz pojedine korisnike pokretne mreže. Hrvatska ima slične razinu penetracije širokopojasnog pristupa Internetu putem pokretne mreže kao i ostatak Europe (tj. ona iznosi 65% u prvom kvartalu 2014. godine) [4].

Brzine prijenosa podataka putem Interneta brzo su rasle u posljednjih deset godina. GPRS (*General Packet Radio Service*) je prva tehnologija koja je omogućila pokretni pristup Internetu, i to brzinama do 114 kbit/s, dok najnovija tehnologija, odnosno dugoročna evolucija pokretne mreže (engl. *Long Term Evolution*, LTE) pruža brzine prijenosa podataka do 300 Mbit/s u dolaznom smjeru i 75 Mbit/s u odlaznom smjeru [5]. Budući da su korisnici u stalnoj potražnji za sve većim količinama podataka [6] te sve više i više njih za širokopojasni pristup Internetu koristi pokretne mreže [1], mrežni operatori pokretnih mreža imaju dovoljno motiva za ulaganje u nove mrežne tehnologije koje će povećati brzinu prijenosa podataka.

U ovom izvješću ćemo pokazati izmjerene vrijednosti brzina prijenosa podataka za pristup Internetu putem mreže LTE jednog od mrežnih operatora u Hrvatskoj. Trenutno mrežni operateri oglašavaju samo maksimalnu brzinu prijenosa podataka. Stoga je cilj ovog izvješća bio utvrditi kolike su stvarne brzine prijenosa podataka u pojedinim područjima, kolika su njena kolebanja te vidjeti koliko se te brzine razlikuju od onih koje reklamiraju operatori. Naime, brzina prijenosa podataka iznimno je značajan faktor u pružanju usluge krajnjem korisniku koji pomaže osiguravanju veće razine kvalitete usluge (engl. *Quality of Service*, QoS) i kvalitete iskustva (engl. *Quality of Experience*, QoE) [7].

U poglavlju 1.3 navedena su osnovna obilježja pokretne mreže LTE, s naglaskom na radijski dio koji ponajviše utječe na brzinu prijenosa podataka iz perspektive krajnjeg korisnika. Poglavlje 1.4. sadrži opis dva alata koji su korišteni pri provedbi mjerenja, dok se u poglavlju 1.5 iznose rezultati mjerenja i njihova analiza. Na kraju, u poglavlju 1.6, daje se zaključak provedenih mjerenja te postavljaju ciljevi za nastavak istraživanja.

### 1.3. Obilježja LTE mreža

Mreža LTE nastavak je stabla 3GPP (*3rd Generation Partnership Project*) pokretnih mrežnih tehnologija započetih s GSM (*Global System for Mobile Communications*), GPRS i EDGE (*Enhanced Data Rates for GSM Evolution*) mrežama, a potom nastavljen s UMTS (*Universal Mobile Telecommunications System*) i HSPA (*High Speed Packet Access*) mrežama. Razvoj LTE-a započinje kroz evoluciju treće generacije (3G) pokretnih mreža krajem 2004. godine. U to vrijeme 3GPP prihvaća specifikaciju IMT-Advanced [8] koju izdaje ITU-R (*International Telecommunication Union - Radiocommunication Sector*) kao osnovu za razvoj vlastite nove (4G) generacije pokretnih mreža. Iako je prva verzija mreže LTE specificirana u izdanju 3GPP Release 8 [9] 2008. godine, ona nije u potpunosti zadovoljavala spomenutu specifikaciju IMT-Advanced. Svi zahtjevi su u potpunosti zadovoljeni tek izlaskom specifikacije 3GPP Release 10 [10] 2011. godine koja definira novu generaciju mreže (LTE-Advanced). Time LTE-Advanced postaje prva u potpunosti funkcionalna i IMT-Advanced kompatibilna 4G pokretna mreža. Međutim, snažan marketing i *branding*, pojačan činjenicom da LTE znatno povećava kapacitet mreže i brzinu prijenosa podataka u odnosu na prethodne generacije pokretnih mreža te koristi modificirano radijsko sučelje s potpuno izmijenjenom jezgrenom mrežom, na kraju nezasluženo titulu 4G mreže vraća natrag LTE-u. Važno je naglasiti da je, osim 3GPP-a [11], 3GPP2 (*3rd Generation Partnership Project 2*) [12] također prihvatio LTE kao nadogradnju svojih CDMA2000 mreža što znači da LTE omogućuje vezu i prekapčanje prema brojnim *legacy* standardima, uključujući GSM/UMTS i CDMA pokretne mreže.

LTE karakterizira pojednostavljena mrežna arhitektura koja u radijskom dijelu sadrži samo eNode-B (evoluirane Node-B) čvorove te posve promijenjena jezgrena mreža koja je zamijenila dotadašnju GPRS jezgrenu mrežu obilježenu prvenstveno prilaznim (engl. *Gateway GPRS Support Node*, GGSN) i uslužnim GPRS potpornim čvorovima (engl. *Serving GPRS Support Node*, SGSN). Nova jezgrena mreža ima nekoliko novih čvorova - MME (*Mobility Management Entity*), SGW (*Serving Gateway*), PGW (*PDN Gateway*) i HSS (*Home Subscriber Server*), a podržava i flat-IP arhitekturu. Štoviše, činjenica da ima manje mrežnih elemenata znači da ima niže operativne troškove i troškove održavanja, te smanjene vrijednosti kašnjenja na korisničkoj i kontrolnoj protokolnoj ravni. MME je središnji upravljački element mreže LTE koji je odgovoran za provjeru autentičnosti korisnika s HSS-om te sudjeluje u izboru SGW-a tijekom početnog spajanja korisničke opreme (engl. *User Equipment*) i tijekom intra-LTE prekapčanja. Također je uključen u proces aktivacije i deaktivacije nosilaca (engl. *bearer*). SGW usmjerava i prosljeđuje podatkovni promet, a također sudjeluje i kao sidro za pokretljivost tijekom inter-eNode-B prekapčanja i prekapčanja između mreže LTE i drugih 3GPP pokretnih mreža. PGW osigurava povezanost s vanjskim paketskim podatkovnim mrežama (npr. Internetom) i obavlja politike pristupa, filtriranja paketa za svakog korisnika, pruža podršku za plaćanje i zakonski utemeljeno presretanje prometa (engl. *lawful interception*). HSS je središnja baza podataka zasnovana na starijim generacijama baza podataka: čvorovima HLR (*Home Location Register*) i AUC (*Authentication Center*). Zadužena je za spremanje podataka o korisnicima i njihovim pretplatama [13].



Razvoj pristupa eUTRA (*evolved UMTS Terrestrial Radio Access*), nadogradnje radijskog sučelja za mrežu LTE, nije bio motiviran samo omogućavanjem većih brzina prijenosa podataka i manjim kašnjenjima, već i većom spektralnom efikasnošću u odnosu na prethodne standarde koji omogućuju operatorima pokretnih mreža pružanje kvalitetnijih usluga i proizvoda. Ključne značajke novog radijskog sučelja, a koje će detaljnije biti pojašnjene u nastavku poglavlja, također su važne za razumijevanje uvjeta u kojima su se odvijala mjerenja koja će biti predstavljena na kraju ovoga izvješća.

*Skalabilni prijenosni pojas:* Kanal u mreži LTE raspolaže s četiri puta većom propusnosti (20 MHz) u dolaznom i odlaznom smjeru u odnosu na UMTS-ovih 5 MHz, a ono što je također važno je da je prilagodljiv. To znači da ako prijenosni pojas od 20 MHz nije dostupan, LTE nudi kanale veličine 1,25, 2,5, 5, 10 ili 15 MHz. Ta karakteristika može poslužiti kao prednost operatorima pokretne mreže koji raspolažu s različitim prijenosnim pojasevima, što im omogućuje da nude različite usluge na temelju raspoloživog spektra. Na višim frekvencijama mreža LTE postaje atraktivna za strategije usredotočene na kapacitet mreže, dok na nižim frekvencijama može omogućiti vrlo dobru i isplativu pokrivenost područja.

*Poboljšana spektralna učinkovitost:* Ovo obilježje odnosi se na to kako pristupni sloj pokretne mreže koristi ograničenu propusnost. Spektralna učinkovitost mreže LTE je 3-4 puta veća u odnosu na mrežu UMTS (Rel6) u dolaznom smjeru i 2-3 puta veća u odlaznom smjeru. Prema tome, LTE omogućuje prijenos veće količine podataka u danom prijenosnom pojasu čime se povećava broj korisnika i usluga koje pokretna mreža može podržati. Primjerice, mreža LTE teoretski podržava najmanje 200 aktivnih korisnika u pojedinoj 5 MHz ćeliji [13].

*Podrška za frekvencijsko i vremensko dupleksiranje:* LTE podržava oba načina dupleksiranja: frekvencijsko (engl. *Frequency-Division Duplex*, FDD) i vremensko (engl. *Time-Division Duplex*, TDD). TDD, kao što mu ime sugerira, dijeli jedan frekvencijski nosilac u naizmjeničnim vremenskim razmacima za prijenos podataka u dolaznom i odlaznom smjeru, dok FDD koristi uparene spektre razdvojene frekvencijskim pojasom. Danas je tipično da isti *chipset* u pokretnom uređaju podržava oba (TDD i FDD) načina rada. Tome ide u prilog i činjenica da, iako oba načina dupleksiranja imaju vlastitu strukturu prijenosnog okvira, oni su međusobno usklađeni pa se slični hardver može koristiti i u baznim stanicama i u pokretnim uređajima.

*Korištenje OFDM modulacijske sheme:* eUTRA koristi OFDM (*Orthogonal Frequency-Division Multiplexing*) kao osnovnu modulacijsku shemu. Modulacijska shema OFDM je izabrana zbog svoje robusnosti u prisutnosti višestaznog slabljenja signala (engl. *multipath fading*). LTE se za razliku od prethodnih generacija pokretnih mreža ne oslanja na povećanje stope simbola kako bi se postigle veće brzine prijenosa podataka. Zauzvrat, koristi OFDM shemu koja dostupni prijenosni pojas „razdvaja“ u niz uži podnosilaca koji prenose podatke u paralelnim tokovima. Svaki podnosilac je moduliran koristeći promjenjivu razinu QAM modulacije (npr. QPSK, 16QAM, 64QAM ili čak i višeg reda, ovisno o kvaliteti signala). To rezultira vrlo učinkovitim korištenjem raspoloživog prijenosnog pojasa, i to praktički bez smetnji među susjednim podnosiocima. OFDM ima i nekoliko slabosti, kao što su osjetljivost na frekvencije nosilaca i velika razina signala PAPR (*Peak-to-Average Power Ratio*).

*Različite tehnike višestrukog pristupa za dolazni i odlazni smjer:* LTE koristi OFDMA (*Orthogonal Frequency-Division Multiple Access*) u dolaznom smjeru i SC-FDMA (*Single-Carrier Frequency-Division Multiple Access*) u odlaznom smjeru. Iako OFDMA uključuje dodatnu složenost u smislu raspoređivanja resursa, riječ je u odnosu na paketski orijentirane pristupe (npr. CSMA (*Carrier Sense Multiple Access*)) i njegov slučajni pristup za smanjenje sudara) superiornoj tehnici višestrukog pristupa u smislu učinkovitosti i kašnjenja. Svakom korisniku dodjeljuje se određeni broj frekvencijskih podnosilaca za unaprijed određeni vremenski iznos, odnosno blok poznat pod kraticom PRB (*Physical Resource Block*). PRB-ovi raspolažu s vremenskom i frekvencijskom dimenzijom, a njihovo raspoređivanje je posao čvorova eNode-B. Negativan učinak takvog pristupa je visoka razina PAPR-a u dolaznom smjeru, što bi u odlaznom smjeru zahtijevalo korištenje skupocjenih pojačala snage. Zbog činjenice da su ograničenja baterija pokretnih uređaja u odlaznom smjeru značajan problem, mreža LTE koristi nešto promijenjenu tehniku višestrukog pristupa u odnosu na OFDMA, ali s vrlo sličnom temeljnom arhitekturom. SC-FDMA nudi isti stupanj zaštite u prisutnosti višestaznog slabljenja signala, ali zbog činjenice da pojedini frekvencijski nosioci nisu samostalno modulirani kao kod OFDMA, postiže se niža razina PAPR-a i time rješava glavni nedostatak osnovnog višestrukog pristupa OFDMA.

*Više-antenske tehnike:* Mreža LTE iskorištava dvije više-antenske tehnike za poboljšanje robusnosti veze i povećanje brzine prijenosa podataka. Tehnika MRC (*Maximal Ratio Combining*) koristi se kako bi se poboljšala pouzdanost veze prilikom niske razine signala i pojave frekvencijski ovisnog slabljenja signala (engl. *frequency selective fading*). To se postiže linearnom kombinacijom kanala čime se nadoknađuje snaga signala što rezultira povećanjem razine signala u odnosu na šum (engl. *Signal-to-Noise Ratio*, SNR). Tehnika MIMO (*Multiple-Input Multiple-Output*), s druge strane, povećava brzinu prijenosa podataka koristeći višestruke antene na prijamnoj i odašiljačkoj strani koje emitiraju/primaju neovisne tokove podataka preko svake od antena (do 4x4). MIMO se može realizirati pomoću jedne od tri navedene metode: predkodiranje (engl. *precoding*), prostorno multipleksiranje (engl. *spatial multiplexing*) i kodiranje raznolikosti (engl. *diversity coding*).

*Podrška za fleksibilnim veličinama ćelija:* LTE podržava femtoćelije s radijusom od svega nekoliko desetaka metara s jedne strane, i velike makroćelije s radijusom od gotovo 100 km s druge strane. Prve se u kombinaciji s višim frekvencijama koriste u gusto naseljenim urbanim područjima, dok su potonje tipične za ruralna područja i karakterizira ih rad na nižim frekvencijama. Štoviše, spektralna učinkovitost u mreži LTE nije poboljšana samo u blizini baznih stanica, već i blizu rubova ćelija, zbog čega se postižu 2-3 puta veće brzine prijenosa podataka u odnosu na prethodne generacije pokretnih mreža.

*Poboljšana podrška za QoS:* Smanjeno kašnjenje (odnosno RTT (*Round Trip Time*) = dvostruko kašnjenje) i smanjeni gubitak paketa ključni su čimbenici u pružanju kvalitetne usluge krajnjim korisnicima, posebice kada je mnogo korisnika aktivno unutar ćelije. Mreža LTE dizajnirana je s ciljanim kašnjenjem manjim od 5 ms u slučaju korisničke i manjim od 100 ms u slučaju kontrolne protokolne ravnine. Time je omogućena bolja podrška za stvarnovremenske aplikacije (npr. strujanje video sadržaja, video konferencije i višekorisničke igre za pokretne uređaje (engl. *multi-player mobile gaming*)).

Brzine prijenosa podataka u mreži LTE prvenstveno ovise o širini korištenog prijenosnog pojasa (1,25 do 20 MHz) i više-antenskih tehnologija (MIMO 2x2, 4x4). S druge strane, na kvalitetu radijskog signala utječu brojni čimbenici, a tipični primjeri su slabljenje signala pri širenju kroz prostor (engl. *free space loss*), prepreke (engl. *diffraction*), prisutstvo višestaznog slabljenja signala (engl. *multipath fading*) i vremenski uvjeti poput kiše ili snijega. To znači da se teoretski maksimumi (tj. 300 Mbit/s u dolaznom smjeru i 75 Mbit/s u odlaznom smjeru) mogu ostvariti samo u idealnim, laboratorijskim uvjetima pri propusnosti od 20 MHz i uz 4x4 MIMO postavku antena. Spomenute vrijednosti, ili općenito bilo koji ostvarivi maksimum brzine prijenosa podataka, ovisno o mrežnim postavkama, gotovo je nemoguće postići u uvjetima koji vladaju u vanjskom svijetu. Glavni razlog tome je činjenica da se mora uzeti u obzir dodatno opterećenje u prijenosu podataka koje je posljedica adaptivnih modulacijskih tehnika i zaštitnog kodiranja koji se pokušavaju nositi s navedenim čimbenicima na kvalitetu radijskog signala te njihovom pogubnom utjecaju na snagu signala [14].

#### 1.4. Mjerni alati

Ovo poglavlje daje opis dva alata koji su korišteni pri mjerenju brzine prijenosa podataka prilikom pristupa Internetu putem pokretne mreže 4G LTE. Prvi program službeni je alat razvijen u HAKOM-u (Hrvatska regulatorna agencija za mrežne djelatnosti) poznat pod nazivom HAKOMETar [15]. Izvorna namjena tog alata je mjerenje brzine prijenosa podataka prilikom fiksnog širokopojsnog pristupa Internetu, i u slučaju ograničenih brzina prijenosa podataka može se rabiti za slanje službenih pritužbi mrežnom operatoru [16]. Međutim, isti se alat može koristiti i za mjerenje brzine prijenosa podataka kod bežičnih ili pokretnih mreža, ali uz ograničenje da se ne može koristiti za slanje službene žalbe. HAKOMETar generira HTTP (*Hypertext Transfer Protocol*) i FTP (*File Transfer Protocol*) promet, a oba se oslanjaju na transportni protokol TCP (*Transmission Control Protocol*) [17].

HAKOMETar na temelju tablica usmjeravanja usmjeritelja na kojeg je spojen nasumično odabire određeni broj poslužitelja i otvara konekcije prema njima kako bi izmjerio brzinu prijenosa podataka. Mjeri brzinu prijenosa podataka u dolaznom smjeru tijekom preuzimanja nekoliko datoteka s poslužitelja (pomoću oba protokola, HTTP i FTP), a na kraju onu višu brzinu od oba protokola u svim mjerenjima odabire kao rezultat mjerenja. U jednom mjernom procesu HAKOMETar generira do 200 MB podatkovnog prometa. Brzina prijenosa podataka u odlaznom smjeru mjeri se samo u prvom koraku mjerenja kada je fokus na mreži između korisnika i mreže CARNet (*Croatian Academic and Research Network* - Hrvatska akademska i istraživačka mreža). Ta brzina nije od interesa za nas jer želimo mjeriti brzinu prijenosa podataka u odlaznom smjeru kada se pristupa poslužiteljima izvan CARNet-ove mreže.

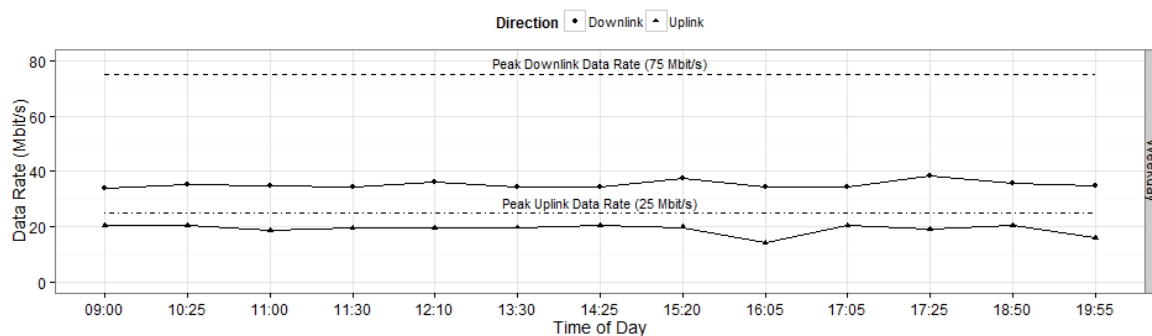
Iz navedenog razloga, za mjerenje brzine prijenosa podataka u odlaznom smjeru korišten je alat Speedtest [18] kojega je razvila tvrtka Ookla. Speedtest djeluje na sljedeći način: pronalazi poslužitelj u blizini te obavlja preuzimanje i slanje slučajnog prometa s odnosno na taj poslužitelj [19]. Istodobno može pokrenuti četiri dretve koje se koriste pri stvaranju konekcija za dolazni i odlazni promet s odabranim poslužiteljem. Za razliku od HAKOMETra, koji mjeri i HTTP i FTP promet i zatim odabire onaj s boljim performansama, Speedtest mjeri samo promet zasnovan na protokolu HTTP. Prilikom provedbe mjerenja primijećeno je da su brzine prijenosa u dolaznom smjeru mjerene pomoću HAKOMETra i Speedtesta vrlo slične.

Dapače, u više od 70% mjerenja razlika brzina prijenosa podataka bila je manja od 2 Mbit/s. Postoje neke razlike u radu ova dva alata, ali to je razumljivo i očekivano, jer nemoguće je pri svakom mjerenju simulirati iste uvjete na mreži ili ih uvijek povezivati s istim poslužiteljima. Rezultati mjerenja koji su prikazani u sljedećem poglavlju dobiveni su na sljedeći način: brzina prijenosa podataka u dolaznom smjeru mjerena je pomoću HAKOMETra, dok je promet u odlaznom smjeru mjereno pomoću alata Speedtest. Za spajanje na Internet posredstvom pokretne mreže korišten je LTE USB modem Alcatel OneTouch L100 [20].

## 1.5. Rezultati

Brzine prijenosa podataka tijekom pokretnog pristupa Internetu mjerene su na četiri lokacije u gradu Zagrebu – četvrtima Trešnjevka sjever, Donja Dubrava i Stenjevec koje predstavljaju dominantno stambena područja, dok četvrt Trnje, gdje se nalazi FER (Fakultet elektrotehnike i računarstva) predstavlja mješovito poslovno i stambeno područje. Sve lokacije u navedenim četvrtima na kojima su obavljena mjerenja pokrivena su signalom pokretne mreže 4G LTE. Dobivene vrijednosti brzina mjerene su pomoću alata opisanih u prethodnom poglavlju - HAKOMETar i Speedtest. Za svaku lokaciju, osim brzine prijenosa podataka, promatra se i razina kolebanja te brzine tijekom dana te se nastoji zaključiti kada je ona viša odnosno niža. Rezultati mjerenja prikazani su odvojeno za radne dane i za vikende. Svaki od grafova prikazuje agregirane vrijednosti brzina prijenosa tijekom sličnih vremenskih trenutaka tijekom radnog dana odnosno vikenda. Apscisa (x-os) na grafovima prikazuje točno vrijeme provedbe mjerenja u danu, dok ordinata (y-os) prikazuje brzinu prijenosa podataka izraženu u Mbit/s.

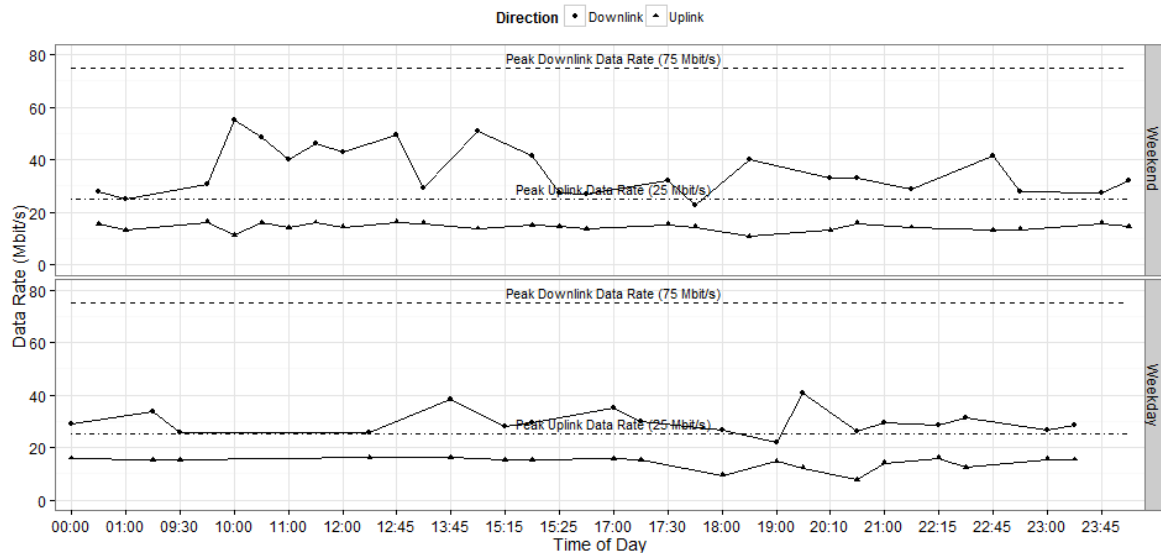
Slika 1 prikazuje brzine prijenosa podataka putem mreže LTE izmjerene na FER-u u četvrti Trnje samo tijekom radnih dana. Trnje pokriva površinu od 7,37 km<sup>2</sup> s gustoćom naseljenosti od 5.737,1 stanovnika po km<sup>2</sup>. Ovo mjesto je specifično po vrlo maloj razini kolebanja brzina. Maksimalna brzina u dolaznom smjeru iznosi 38 Mbit/s, a minimalna 34 Mbit/s, dok je u odlaznom smjeru ta razlika nešto veća - od maksimalnih 21 Mbit/s do minimalnih 14 Mbit/s.



Slika 1. Rezultati mjerenja za lokaciju „FER“ u četvrti „Trnje“

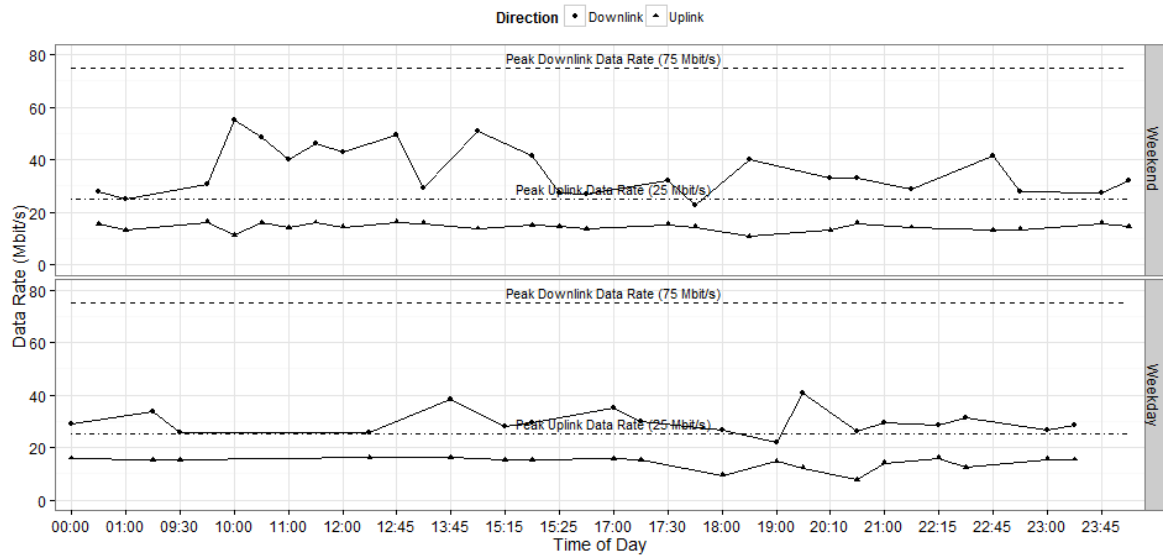
Vrijednosti izmjerene radnim danom i vikendom u četvrti Donja Dubrava, koja pokriva površinu od 10,82 km<sup>2</sup> s gustoćom naseljenosti od 3.321,1 stanovnika po km<sup>2</sup>, prikazane su na

slici 2. Može se primijetiti da je brzina prijenosa u dolaznom smjeru najviša vikendom prijevodne te da ne postoji puno kolebanja tijekom dana. Brzina prijenosa podataka u dolaznom smjeru varira između 55 Mbit/s i 22 Mbit/s, a u odlaznom smjeru od 16 Mbit/s do 8 Mbit/s.



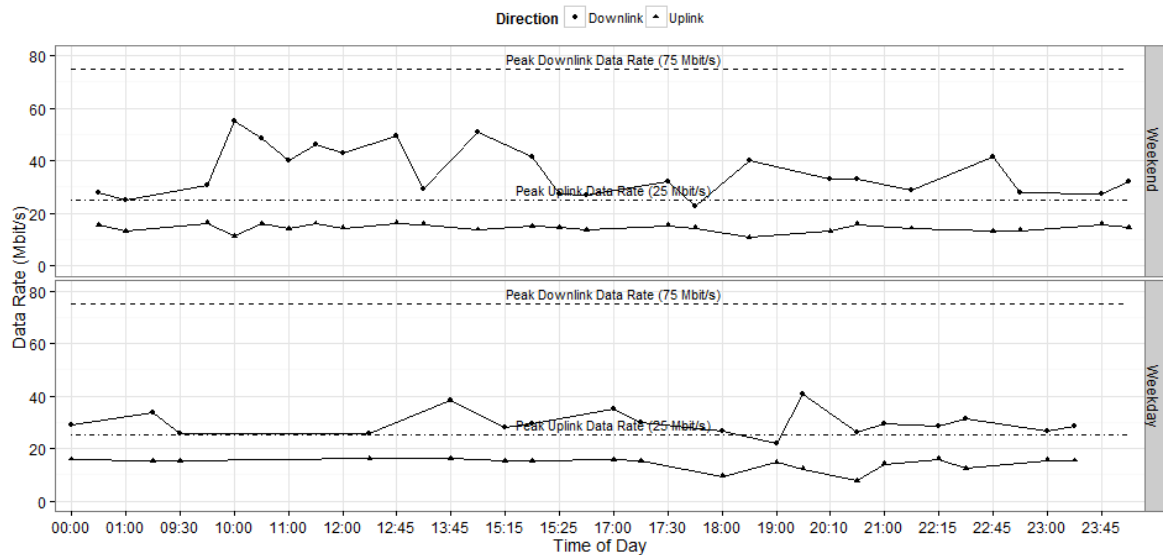
Slika 2. Rezultati mjerenja za lokaciju u četvrti „Donja Dubrava“

Mjerenja provedena na lokaciji Špansko u četvrti Stenjevec, kao što se može vidjeti na slici 3, karakteriziraju nešto manja kolebanja u odnosu na Donju Dubravu. Četvrt Stenjevec pokriva površinu od 12,8 km<sup>2</sup> s gustoćom naseljenosti od 3.387,3 stanovnika po km<sup>2</sup>. Maksimalna brzina prijenosa podataka u dolaznom smjeru je 53 Mbit/s, a minimalna 20 Mbit/s, dok je za odlazni smjer najveća izmjerena vrijednost 16 Mbit/s, a najmanja svega 7 Mbit/s. Može se primijetiti da su brzine prijenosa podataka nešto više tijekom vikenda, kada je i postignuta maksimalna vrijednost.



Slika 3. Rezultati mjerenja za lokaciju u četvrti „Stenjevec“

Konačno, slika 4 prikazuje mjerenja provedena u četvrti Trešnjevka sjever koja obuhvaća područje od 5,83 km<sup>2</sup> s najvećom gustoćom naseljenosti od svih promatranih područja od 9.506,86 stanovnika po km<sup>2</sup>. Rezultati mjerenja su ovdje sasvim drugačiji od drugih lokacija. Maksimalna brzina prijenosa podataka u dolaznom smjeru iznosi svega 27 Mbit/s, a minimalna 14 Mbit/s. Brzine u odlaznom smjeru variraju između 19 Mbit/s i 5 Mbit/s, što je primjer najveće razine kolebanja od svih provedenih mjerenja. Kao i na prethodnim lokacijama, brzine prijenosa podataka tijekom vikenda nešto su veće nego tijekom radnog dijela tjedna, pogotovo u popodnevnim satima.



Slika 4. Rezultati mjerenja za lokaciju u četvrti „Trešnjevka sjever“

Tablica 1 prikazuje vrijednosti medijana brzine prijenosa podataka za dolazni i odlazni smjer za svaku pojedinu lokaciju, zajedno s vrijednostima standardne devijacije, postotak odstupanja te najmanje i najveće izmjerene vrijednosti. Medijan je izabran zbog neregularne i

pomaknute raspodjele vrijednosti provedenih mjerenja, pa nešto preciznije opisuje trend prosječnih vrijednosti mjerenja od jednostavnog prosjeka. Standardna devijacija i njen postotak u odnosu na medijan pokazuju razinu kolebanja izmjerenih vrijednosti brzina. Najviša i najniža izmjerena vrijednost pokazuju raspon brzina prijenosa podataka u kojem su se odvijala mjerenja. Prilikom računanja medijana, brzine prijenosa podataka za vikende i radne dane agregirane su zajedno za svaku od lokacija.

**Tablica 1. Osnovni statistički podaci provedenih mjerenja**

Lokacija	Smjer	Median	StDev	Max	Min	% StDev
Donja Dubrava	Dolazni	29,77	8,24	55,00	22,04	27.69 %
	Odlazni	15,12	1,88	16,21	7,78	12.42 %
FER (Trnje)	Dolazni	34,78	1,29	38,29	34,06	3.71 %
	Odlazni	19,73	1,89	20,50	14,27	9.58 %
Stenjevec	Dolazni	32,94	8,81	54,17	16,07	26.76 %
	Odlazni	5,71	3,98	18,31	1,59	69.69 %
Trešnjevka sjever	Dolazni	16,98	4,92	25,97	7,82	28.98 %
	Odlazni	9,89	4,95	19,16	4,47	50.01 %

Kao što se može primijetiti iz tablice i grafova, najviša prosječna brzina prijenosa podataka u dolaznom smjeru postignuta je na FER-u, nakon čega slijede lokacije u Stenjevcu, Donjoj Dubravi i Trešnjevci sjever. Najveća prosječna brzina u odlaznom smjeru također je vezana uz FER, nakon čega slijede Stenjevec, Trešnjevka Sjever i Donja Dubrava. Nadalje, pojedinačna maksimalna vrijednost u dolaznom smjeru zabilježena je u Donjoj Dubravi, a u odlaznom smjeru na lokaciji FER u četvrti Trnje. Minimalna pojedinačna brzina prijenosa u dolaznom smjeru zabilježena je u četvrti Trešnjevka sjever, dok je za odlazni smjer ona postignuta u Stenjevcu. Najviša prosječna brzina prijenosa podataka postignuta na FER-u može se objasniti činjenicom da se FER nalazi u poslovnoj zoni s brojnim tvrtkama u okružju i stoga povećanom potrebom korisnika tijekom radnog dana, pa su mrežni operatori prilagodili pokrivenost i kapacitet svojih pokretnih mreža sukladno tim zahtjevima. Također, općenito najniže izmjerene vrijednosti, kao i najveća kolebanja u pristupnim brzinama zabilježena su u Stenjevcu i Trešnjevci sjever, snažno urbaniziranim i gusto naseljenim četvrtima. Međutim, potrebno je provesti sustavna mjerenja na više različitih lokacija i kroz odgovarajuće vremensko razdoblje kako bi se mogli potvrditi takvi zaključci ili možda donijeti neki novi.

## 1.6. Zaključak

U ovom izvješću prikazani su rezultati testiranja brzine prijenosa podataka za jednog mrežnog operatora u Hrvatskoj koji omogućuje pristup Internetu putem mreže LTE. Kao što se može zaključiti iz prikazanih rezultata brzine prijenosa podataka, koje su izmjerene pomoću aplikacija HAKOMetar i Speedtest, mijenjaju se tijekom dana s različitim amplitudama na različitim lokacijama u četiri četvrti u gradu Zagrebu. Izmjerene brzine prijenosa podataka promatrane su u dva različita konteksta, radni dan i vikend, a zaključak je da su u dolaznom smjeru brzine općenito nešto više tijekom vikenda. Također, na nekim lokacijama su postignute više brzine prijenosa podataka u jutarnjim satima, na drugima tijekom poslijepodneva, dok su brzine u odlaznom smjeru manje-više stabilne bez obzira na doba dana. Kako bi se mogli donijeti valjani zaključci, potrebno je provesti sustavno mjerenje s većim brojem ponavljanja.

Operatori pokretnih mreža oglašavaju samo maksimalne brzine prijenosa podataka koje se mogu postići preko njihove mreže (u promatranom slučaju to je značilo 75 Mbit/s za dolazni i 25 Mbit/s za odlazni smjer). Te vrijednosti, kako se i očekivalo, nisu postignute u niti jednom od provedenih mjerenja. Najveća izmjerena brzina u dolaznom smjeru u svim provedenim mjerenjima iznosila je 55 Mbit/s, što je za 20 Mbit/s (gotovo 25%) manje od deklarirane vrijednosti koja bi se mogla postići u idealnim uvjetima. S ciljem boljeg informiranja pretplatnika pokretne mreže, preporučujemo da operatori pokretne mreže umjesto dosadašnje prakse oglašavaju prosječnu i maksimalnu brzinu prijenosa podataka prilikom pristupa Internetu koja se može postići na određenom području. Međutim, prije nego je objavljivanje spomenutih podataka moguće, potrebno je ustanoviti sveobuhvatan i sustavni pristup mjerenja na točno određenim lokacijama u zadanim vremenskim intervalima, tako da dobiveni rezultati budu u korelaciji sa stvarnim uvjetima u mreži.



## 1.7. Literatura

- [1] “ICT Facts and Figures - The World in 2013,” International Telecommunication Union (ITU), February 2013.
- [2] “ICT Statistics,” International Telecommunication Union (ITU), February 2014.
- [3] “ICT Facts and Figures - The World in 2014,” International Telecommunication Union (ITU), April 2014.
- [4] “Mobile broadband penetration (all active users),” Croatian Regulatory Authority for Network Industries (HAKOM), April 2014.
- [5] “3GPP The Mobile Broadband Standard - LTE, <http://www.3gpp.org/technologies/keywords-acronyms/98-lte>,” visited on July 2, 2014.
- [6] “The Mobile Economy 2013,” AT&Kearney, GSMA, 2014.
- [7] D. Staehle, K. Leibnitz, and K. Tsipotis, “QoS of Internet Access with GPRS,” in Proceedings of the 4th ACM International Workshop on Modeling, Analysis and Simulation of Wireless and Mobile Systems. New York, NY, USA: ACM, 2001, pp. 57–64.
- [8] “ITU Global Standard For International Mobile Telecommunications ”IMT-Advanced”, <http://www.itu.int/ITU-R/index.asp?category=information&mlink=imt-advanced&lang=en>,” visited on June 26, 2014.
- [9] “3GPP Release 8, <http://www.3gpp.org/specifications/releases/72-release-8>,” visited on June 26, 2014.
- [10] “3GPP Release 10, <http://www.3gpp.org/specifications/releases/70-release-10>,” visited on June 26, 2014.
- [11] “About 3GPP Home, <http://www.3gpp.org/about-3gpp/about-3gpp>,” visited on June 26, 2014.
- [12] “About 3GPP2, [http://www.3gpp2.org/Public\\_html/Misc/AboutHome.cfm](http://www.3gpp2.org/Public_html/Misc/AboutHome.cfm),” visited on June 26, 2014.
- [13] U. Forum, Towards Global Mobile Broadband: Standardising the future of mobile communications with LTE (Long Term Evolution), 2008.
- [14] Motorola, Realistic LTE Performance: From Peak Rate to Subscriber Experience, 2009.
- [15] “Hakometar, [www.hakom.hr/default.aspx?ID=1144](http://www.hakom.hr/default.aspx?ID=1144),” visited on June 26, 2014.
- [16] M. Weber, V. Svedek, Z. Jukic, I. Golub, and T. Zuljevic, “Can HAKOMETAR be used to increase transparency in the context of network neutrality?” in Telecommunications (ConTEL), 2013 12th International Conference on, June 2013, pp. 309–316.

[17] “Quality of Service Analysis in Broadband Internet Access,” Croatian Regulatory Authority for Network Industries, March 2014.

[18] “Speedtest, [www.speedtest.net](http://www.speedtest.net),” visited on June 26, 2014.

[19] “Knowledge Base - How Speedtest.net works, <https://support.speedtest.net/forums/20483933-How-Speedtest-net-works>,” visited on July 8, 2014.

[20] “Alcatel onetouch L100, <http://www.alcatelonetouch.com/globalen/products/mobile-broadband/one-touch-l100v.html.U7-0Z7Hb64c>,” visited on July 11, 2014.

## **2. Prijetnje korisnicima telekomunikacijskih usluga i kalkulator za procjenu rizika povrede privatnosti korisnika**

### **1.1. Uvod**

Ubrzanim razvojem informacijskog društva dolazi do razvoja novih, naprednijih digitalnih tehnologija koje postaju dio javne komunikacijske mreže. Ovaj proces za sobom povlači potencijalne opasnosti povezane sa zaštitom osobnih podataka i privatnosti korisnika.

Internet mijenja tradicionalne tržišne strukture pružajući zajedničku globalnu infrastrukturu za pružanje širokog raspona elektroničkih komunikacijskih usluga. Javno dostupne elektroničke komunikacijske usluge putem Interneta otvaraju korisnicima nove mogućnosti, ali također i nove opasnosti za njihovu sigurnost i privatnost. Postoje mnogi poznati slučajevi povrede privatnosti na Internetu koji upozoravaju kako to postaje sve veći problem u današnjem društvu. Problemom privatnosti na Internetu intenzivno se počelo baviti nakon razvoja mnoštva aplikacija kao što su: društvene mreže, e-kupovina, itd. na kojima korisnici ostavljaju veliki broj privatnih informacija. Privatnost na Internetu teško je postići zbog interaktivnosti korisnika i pružatelja usluge pristupa Internetu te njegovog neprekidnog razvoja.

Korisnici sve više postaju neoprezni, ne razmišljaju o opasnostima koje prijete na Internetu.

Davatelji usluga trebaju poduzeti odgovarajuće mjere s ciljem zaštite sigurnosti njihovih usluga te obavijestiti pretplatnike o posebnim opasnostima proboja sigurnosti mreže. Posebno je važno za korisnike da ih njihov davatelj usluga u potpunosti obavijesti o postojećim sigurnosnim opasnostima koje leže izvan opsega mogućih sredstava za otklanjanje opasnosti koje davatelj usluga može pružiti.

Ovaj rad je uvod u brošuru i aplikaciju koja će nastati iz suradnje FER-a i HAKOM-a, a cilj je korisnike upoznati s mogućim opasnostima te potaknuti stručnu javnost za potrebe novih pogleda i stvaranja novih regulatornih okvira privatnosti na Internetu.

U poglavlju 1.2 navedene su prijetnje s kojima se korisnici mogu najčešće susresti na Internetu, dok poglavlje 1.3 daje savjete za izbjegavanje internetskih prijevara. U poglavlju 1.4 opisuju se scenariji u kojima korisnici svojevolumno ostavljaju podatke na različitim web-uslugama. Poglavlje 1.5 donosi opis kalkulatora zasnovanog na neuronskim mrežama koji procjenjuje rizik povrede privatnosti korisnika.

## 1.2. Najčešće prijetnje

U ovom poglavlju se opisuju najčešće prijetnje kojima su izloženi korisnici Interneta preko svog e-mail računa, računa na društvenim mrežama ili podataka koje ostavljaju na drugim stranicama poput e-trgovine.

**PRIJETNJA:** Phishing [1]

**KORIŠTENI PARAMETRI:** e-mail adresa

**OPIS:** *Phishing* prijevare zasnivaju se na slanju lažnih e-mail poruka putem kojih se nastoje prikupiti povjerljivi podaci o bankovnim računima, kreditnim karticama i sl. Najčešći oblik *phishinga* podrazumijeva lažnu e-mail poruku koja imitira službeni zahtjev financijske institucije (npr. banke ili osiguravajućeg društva) o promjeni podataka korisnika i sadrži poveznicu na njenu lažnu web-stranicu putem koje žrtva, nesvjesna da se radi o prijeveri, popunjava obrazac povjerljivim podacima (korisničko ime i lozinka za pristup računu, brojevi kreditnih kartica, ali i ostali osobni podaci poput adrese stanovanja, JMBG-a/OIB-a itd.). Varijacije prijeverare traže od potencijalne žrtve slanje povratne e-mail poruke s povjerljivim podacima ili uključuju privitke zaražene *malwareom* putem kojih napadači dobivaju tajni pristup žrtvinom računalu, što znači da mogu presretati sve podatke koje žrtva izmjenjuje preko Interneta. *Phishing* prijeverare u pravilu nisu personalizirane pa vrlo rijetko potencijalnu žrtvu usmjeravaju prema lažnoj web-stranici institucije kojoj stvarno i pripada. Međutim, napadači se oslanjaju na zakon velikih brojeva, tako da manji dio poslanih poruka u potpunosti pogodi kontekst za uspješnu prijeveru.

**POSLJEDICE:** Napadači prikupljanjem povjerljivih podataka mogu preuzeti kontrolu nad bankovnim računom žrtve, podatke za korištenje kreditne kartice, a u nekim ozbiljnijim varijantama, ako su uspjeli prikupiti dovoljno osobnih podataka, čak i identitet žrtve. Preuzimanje bankovnog računa znači da imaju potpunu kontrolu nad novcima i mogu ih vrlo lako prenijeti na neki drugi račun. Slična je situacija s preuzetom kreditnom karticom, pomoću koje napadači najčešće u vrlo kratkom roku obavljaju razne transakcije dok god ima novaca na raspolaganju. U tim je slučajevima najbitnije u što kraćem roku o krađi obavijestiti nadležnu financijsku instituciju koja onda poduzima odgovarajuće protumjere. U slučajevima krađe identiteta, posljedice mogu biti puno dugotrajnije te žrtve ponekad potroše mjesec ili čak godine kako bi „očistili“ svoje ime, riješili sve pravne sporove i oporavili se od nagomilanih dugova.

**PRIJETNJA:** Nigerian Scams [2]

**KORIŠTENI PARAMETRI:** e-mail adresa, profil društvene mreže

**OPIS:** Nigerijske prijeverare započele su još u vremenima „papirnatih“ pošte, no pravi su zamah doživjele kada je pošta prešla u sferu elektroničke komunikacije. Danas je elektronička pošta najčešći medij za širenje ovakvih prijevera, iako postupno prelaze i u domenu društvenih

mreža. Bez obzira na naziv, napadači koji se koriste s ovom vrstom prijevare ne moraju nužno dolaziti iz Nigerije. Ovakve prijevare, bez obzira na priču u pozadini, zasnivaju se na zahtjevu za pomoć pri prebacivanju velike svote novaca s međunarodnog bankovnog računa, a što napadač zbog raznolikih razloga (zakonskih ograničenja, korupcije, bolesti, itd.) nije u stanju sam učiniti. Pozadinske priče mogu biti raznolike: od zahtjeva za prebacivanje velike svote novaca s računa umirućeg milijardera u dobrotvorne svrhe, problema s koruptivnom diktatorskom vlašću koja sprečava napadače u prebacivanju novaca u inozemstvo, do tvrdnje da ste upravo vi jedini živi nasljednik preminulog bogatog industrijalca koji može pristupiti njegovom bankovnom računu. Posebno raširena varijacija ove prijevare su obavijesti o glavnom dobitku na nagradnoj igri/lotu. Žrtvama koje povjeruju u priču kako će za svoje sudjelovanje u poslu dobiti izdašnu naknadu vrlo brzo dolazi novi zahtjev putem e-maila za uplatom manje svote novaca kako bi se platili pravni troškovi ili podmitili korumpirani lokalni dužnosnici prije nego li se nastavi s dogovorenim poslom. Međutim, nastavak posla dakako ne postoji jer se cijela prijevarena zasnivala na uvjeravanju žrtve kako je nužno unaprijed uplatiti naknadu za pravne troškove jer će joj se u nastavku posla vratiti višestruki iznos.

**POSLJEDICE:** Najčešća posljedica za naivne žrtve koje su odlučile unaprijed uplatiti novac za nastavak posla je gubitak tih novaca. U nekim situacijama se od žrtvi traže povjerljivi osobni i/ili bankovni podaci, tako da je moguć scenarij u kojem napadači preuzimaju kontrolu nad bankovnim računima i kreditnim karticama. Nažalost, u nekim ozbiljnijim situacijama su se dogodile otmice, pa čak i ubojstva žrtvi koje su pristale sudjelovati u prijevarama ove vrste. Prema tome, najbitnije je ne nasjedati na ovakve e-mail ponude i ne ostvarivati ikakav kontakt s napadačima jer posljedice kako je praksa pokazala, nažalost mogu biti tragične.

**PRIJETNJA:** Payment Transfer Job [3]

**KORIŠTENI PARAMETRI:** e-mail adresa

**OPIS:** Ove vrste prijevare uvelike podsjećaju na Nigerijske prijevare, ali svejedno ih odlikuje nekoliko specifičnosti zbog čega ih se svrstava u posebnu kategoriju. Scenarij je slijedeći: na e-mail adresu potencijalne žrtve dolazi zahtjev za pomoć pri prebacivanju velike svote novaca na bankovni račun žrtve koja ga je dužna dalje prosljediti na unaprijed dogovoreni račun, uz dakako pravo zadržavanja dijela sredstava kao naknade za obavljene posao. Najčešći razlozi koji napadača, a koji se vrlo često predstavljaju kao međunarodna kompanija, sprečavaju da samostalno prebace novac su pravne zavrzlake ili problemi pri pretvorbi valuta u banci. U pozadini priče se najčešće krije „prljavi novac“ kojega napadači pomoću naivnosti žrtve pokušavaju „oprati“ i na taj način otežati posao policiji u praćenju novca. Novac koji napadači na ovaj način pokušavaju sakriti od organa zakona i reda najčešće je rezultat drugih uspješnih prijevora poput *phishinga*, nigerijskih prijevora, lažnih *online* prodaja i sl. Žrtva koja pristane sudjelovati u ovakvoj vrsti transakcije vrlo često jedina izvlači deblji kraj: policija i obavještajne agencije redovito prate i traže prijenose ilegalno stečenog novca, pa je vrlo izvjesna situacija da se policija pojavi na vratima baš u onom trenutku kada je ukradeni novac na žrtvinom računu.

**POSLJEDICE:** Žrtva koja je uhvaćena s ukradenim novcem na računu može se suočiti s vrlo ozbiljnim optužbama za sudjelovanje u organiziranom kriminalu te je potrebno puno vremena i novaca kako bi se skinula ljaga s imena te namirili svi pravni troškovi.

**PRIJETNJA:** Pharming [4]

**KORIŠTENI PARAMETRI:** web-pretraživač

**OPIS:** Ova prijevarena se vrlo često brka s *phishingom*, a ponekad se smatra i samo evolucijom *phishing* kategorije prijevarena. Međutim, za razliku od kombinacije lažne e-mail poruke i lažne web-stranice koji su postali zaštitni znak *phishinga*, *pharming* se zasniva na preuzimanju kontrole web-pretraživača koji onda neprimjetno preusmjerava žrtvu na lažnu web-stranicu, najčešće financijskih institucija poput banaka ili osiguravajućih društava. Zbog činjenice da više nema potrebe za navlačenjem žrtvi putem ponekad očiglednih lažnih e-mail poruka, ovakve se prijave smatraju znatno opasnijima za krajnje korisnike.

**POSLJEDICE:** Posljedice su srodne onima iz *phishing* kategorije prijevarena. Napadači prikupljanjem povjerljivih podataka koje žrtva izmjenjuje s lažnom web-stranicom banke mogu preuzeti kontrolu nad bankovnim računom žrtve, podatke za korištenje kreditne kartice, a u nekim ozbiljnijim varijantama, ako su uspjeli prikupiti dovoljno osobnih podataka, čak i identitet žrtve. U slučajevima krađe bankovnih računa i kreditnih kartica najbitnije je u što kraćem roku o krađi obavijestiti nadležnu financijsku instituciju koja onda poduzima odgovarajuće protumjere. Kod krađe identiteta je situacija tipično nešto zamršenija jer se mora obavijestiti veći broj institucija koje su pogođene ovom vrstom prijave.

**PRIJETNJA:** Internet Dating Scams [5]

**KORIŠTENI PARAMETRI:** *online*-usluga za spojeve, e-mail adresa, profil društvene mreže

**OPIS:** Rast popularnosti online usluga za spojeve potaknuo je razvoj ove specifične vrste prijave. Napadač otvara lažni profil na usluzi za spojeve putem kojeg nastoji namamiti potencijalne žrtve. Kada napadač pridobije naklonost žrtve, oni krenu sve češće komunicirati te se uskoro prebacuju na druge komunikacijske medije poput e-maila i društvenih mreža. Uskoro krenu razmjenivati fotografije, pričati o temama iz svakodnevnog života, poput obitelji, zanimljivostima s posla/škole, intime i sl. Cilj je stvoriti iluziju da je riječ o iskrenom i stvarnom odnosu. Kako se približava trenutak potencijalnog susreta uživo, napadač tipično traži novac za kupnju avionske karte kako bi mogao doći na susret, no naravno nikada ne stiže. Postoji više varijacija na temu, pa napadač može tražiti novac ne samo za put, nego i za liječenje bolesnog člana obitelji, pokretanje poslovne ideje i sl. Napadač održava odnos dok god uspješno dobiva novac od žrtve.

**POSLJEDICE:** Tipične žrtve su povučeni i sramežljivi ljudi koji postupno nastoje izgraditi iskren odnos s drugom osobom, no koji nakon ovakvog iskustva, osim očiglednog gubitka novaca koje su nepovratno utrošili na svog lažnog prijatelja/icu, mogu doživjeti i puno teže psihičke posljedice. Treba imati na umu da napadači osim novca mogu zahtijevati i različite povjerljive podatke, poput pristupa bankovnom računu ili kreditnoj kartici. Kada se prijevara razotkrije, sukladno tome koje je sve podatke žrtva prosljedila napadaču, treba uslijediti i adekvatna reakcija: obavijestiti nadležne financijske institucije da je došlo do krađe podataka.

**PRIJETNJA:** Lottery Scams [6]

**KORIŠTENI PARAMETRI:** e-mail adresa

**OPIS:** Ova prijevara je varijacija poznate nigerijske prijevare. Potencijalnu žrtvu se putem e-maila obavještava o dobitku nagrade (velika svota novaca, automobil, kuća na predivnoj lokaciji na Karibima i sl.) koju trebaju preuzeti. Obećana nagrada naravno ne postoji. Međutim, da bi preuzimanje te fiktivne nagrade bilo moguće, prvo se traže kopije raznolikih osobnih dokumenata, poput osobne iskaznice, JMBG-a/OIB-a, vozačke dozvole, putovnice i sl. Razlog tome je tobože provjera identiteta dobitnika nagrade. Također, vrlo često se zahtijeva i plaćanje naknade kako bi novac bilo moguće prebaciti s dakako fiktivnog bankovnog računa. Žrtve koje nasjednu na ovakvu prijevaru najčešće se susreću s krađom identiteta.

**POSLJEDICE:** Posljedice mogu biti vrlo raznolike, a tipično ih karakterizira dugotrajna i iscrpljujuća pravna borba s različitim institucijama koje su oštećene u procesu krađe identiteta kako bi se dokazalo tko je tko i tko je odgovoran za što.

**PRIJETNJA:** Instalacija virusa putem ponude novih aplikacija [7]

**KORIŠTENI PARAMETRI:** korisnički račun na društvenoj mreži s mogućnošću primanja poruka od bilo koga

**OPIS:** Na društvenim mrežama poput Facebooka korisnicima mogu slati poruke i oni korisnici koji nisu na njihovoj listi prijatelja. Neke od tih poruka mogu nuditi npr. stari izgled Facebooka, WhatsApp aplikaciju za desktop, ili video preglednik koji je potreban za gledanje određenog videa. U svakom slučaju, nudi se nešto za što napadači smatraju da će biti veliki interes, i da će korisnici biti voljni instalirati. Instalirani program neće biti ono što se predstavlja, nego virus koji će onda moći pristupiti računalu i svemu što se na njemu nalazi. Korisnika će se najlakše potaknuti da instalira nešto ako mu to preporuči prijatelj, pa je upravo zbog toga prevarantima zanimljiva krađa korisničkih računa. Zbog toga treba paziti što se pokreće, pogotovo ako su to neke aplikacije za koje nismo sigurni što su.

**POSLJEDICE:** Moguća je instalacija različitih virusa koji mogu ukrasti lozinke, podatke o karticama i slično što je već pohranjeno na računalu.

**PRIJETNJA:** Krađa novaca - lažne ponude [8]

**KORIŠTENI PARAMETRI:** korisnički račun na društvenoj mreži s mogućnošću primanja poruka od bilo koga

**OPIS:** Na društvenim mrežama poput Facebooka korisnicima mogu slati poruke i oni korisnici koji nisu na njihovoj listi prijatelja. Na taj način korisnicima se može ponuditi brza zarada uplaćivanjem određenog iznosa na predstavljeni račun, uz obećanje dobiti na investiciju od 2-3%. Štoviše, korisnicima se nudi i veća dobit ako prijateljima na društvenoj mreži preporuče ovaj način investiranja. Novi korisnici koji dobiju preporuku od svojih prijatelja će prije povjerovati da mogu na ovaj način zaraditi. Na kraju, uplaćen novac se preusmjerava na *offshore račune* i korisnici naravno ne dobivaju ništa.

**POSLJEDICE:** Gubitak novca.

**PRIJETNJA:** Krađa novaca - lažne stranice za e-kupovinu [9]

**KORIŠTENI PARAMETRI:** korisnički račun na društvenoj mreži s mogućnošću primanja poruka od bilo koga

**OPIS:** Na društvenim mrežama poput Facebooka korisnicima mogu slati poruke i oni korisnici koji nisu na njihovoj listi prijatelja. Korisnicima se tim kanalima mogu preporučiti i lažne stranice, između ostalog i stranice za e-kupovinu na kojima se može obaviti kupnja, a naravno bez da se tražena roba ikad dobije. Treba biti oprezan u slučajevima kad nepoznata osoba preporuča web-stranice preko kojih se izvršavaju poslovne transakcije.

**POSLJEDICE:** Gubitak novca, mogućnost ostavljanja podataka o karticama koji se kasnije mogu zlorabiti.

**PRIJETNJA:** Lažne poruke u kojima se spominju prijatelji [10]

**KORIŠTENI PARAMETRI:** korisnički račun na društvenoj mreži s mogućnošću primanja poruka od bilo koga

**OPIS:** Na društvenim mrežama poput Facebooka korisnicima mogu slati poruke i oni korisnici koji nisu na njihovoj listi prijatelja. Ako su prijatelji korisnika javno objavljeni, odnosno može ih vidjeti svaki korisnik društvene mreže, prevarant se može praviti da ima određene informacije o Vašem prijatelju koji je u nevolji. Takve poruke najčešće sadrže poveznicu na stranicu koja izgleda kao Facebook na kojoj se traži unošenje podataka za prijavu. Na taj način prevarant zapravo dobiva pristup Vašem računu za društvenu mrežu i na temelju toga može izvršavati nove prijave. Pazite na koje stranice unosite svoje podatke, posebno ako ste na te stranice preusmjereni porukama nepoznatih ljudi!



**POSLJEDICE:** Krađa korisničkog računa na društvenim mrežama, gubitak privatnosti; prevaranti mogu vidjeti sve što se objavljuje, ali i dodavati sadržaj te koristiti račun za daljnje prijevare.

**PRIJETNJA:** Ponuda novih *gadgeta* ili zanimljivog sadržaja [11]

**KORIŠTENI PARAMETRI:** korisnički račun na društvenoj mreži s mogućnošću primanja poruka od bilo koga

**OPIS:** Na društvenim mrežama poput Facebooka korisnicima mogu slati poruke i oni korisnici koji nisu na njihovoj listi prijatelja. Tako se prevaranti mogu predstaviti kao predstavnici neke tehnološke kompanije (npr. Apple) i nuditi najnovije proizvode. Klikom na poveznicu u poruci, korisnika se preusmjerava na web-stranicu na kojoj se zahtijeva upisivanje korisničkog računa i lozinke za Facebook koji zatim služe prevarantima za izvođenje daljnjih prijevara. Mamac za klik na stranicu gdje se zahtijevaju korisnički podaci može biti i neki video za koji prevarant procjenjuje da bi mogao biti zanimljiv širem krugu korisnika. Ne upisujte svoje korisničke podatke na stranice na koje vas se preusmjerava u porukama s nepoznatim pošiljateljima premda one izgledaju isto kao i stranice društvenih mreža.

**POSLJEDICE:** Krađa korisničkog računa na društvenim mrežama, gubitak privatnosti; prevaranti mogu vidjeti sve što se objavljuje, ali i dodavati sadržaj te koristiti račun za daljnje prijevare.

**PRIJETNJA:** Poziv za pregled zanimljivih stranica [12]

**KORIŠTENI PARAMETRI:** korisnički račun na društvenoj mreži s mogućnošću primanja poruka od bilo koga

**OPIS:** Na društvenim mrežama poput Facebooka korisnicima mogu slati poruke i oni korisnici koji nisu na njihovoj listi prijatelja. Prevaranti tako šalju poziv za pregled „zanimljivih“ stranica na kojima se nalaze virusi koji korisnici mogu lako skinuti i pokrenuti na korisničkom računalu ako nisu pažljivi.

**POSLJEDICE:** Moguće je pokretanje virusa koji mogu imati različite mogućnosti – krađu korisničkih računa i lozinke, praćenje svih aktivnosti na računalu, pa tako i podataka za e-bankarstvo.

**PRIJETNJA:** Trajno članstvo u e-trgovinama

**KORIŠTENI PARAMETRI:** ime, prezime, podaci za plaćanje

**OPIS:** Korisnica je kupila robu sa web-stranice trgovine i nikada više nije posjetila ovu stranicu. Nakon osam mjeseci se vratila iz države gdje je studirala u svoju državu. Tada je saznala da joj je s računa (onog s kojeg je prebacila novce za kupovinu navedene robe) svaki mjesec skidana određena svota novca. Nakon toga je malo istraživala po Internetu i saznala da stranica na kojoj je kupila robu funkcionira na sljedeći način: jednom kada se kupi nešto s njihove web-stranice, postajete njihov „VIP član“ bez vašeg znanja. Nakon toga je potrebno da se prijavite na ovu web-stranicu između 1.og i 5.og svaki mjesec i kliknete „preskoči ovaj mjesec“. Ako se ovo ne učini, svaki mjesec će se naplaćivati određena svota novca. U Općim uvjetima poslovanja je navedena stavka: prilikom jedne kupnje postajete VIP član i ako od 1.og i 5.og u mjesecu ne otkazete članstvo to vam se i dalje naplaćuje.

**POSLJEDICE:** Skidanje novaca s računa. Potrebno je proučiti uvjete poslovanja ili bar pročitati recenzije bivših korisnika pri davanju podataka o plaćanju različitim stranicama za e-trgovinu.

### 1.3. Savjeti za izbjegavanje internetskih prijevara

1. Vodite računa o tome da je vatrozid (engl. *firewall*) na vašem računalu uvijek upaljen te redovito instalirajte nadogradnje operativnog sustava, antivirusnog softvera i drugih sigurnosnih programa.
2. Redovito radite kopije podataka i pohranjujte ih na neko sigurno mjesto.
3. Nemojte brzopleta povjerovati svemu što saznate na Internetu.
4. Čuvajte se svega što vam se nudi “besplatno” i izbjegavajte web-stranice koje prodaju proizvode po pretjerano niskim cijenama. To bi mogla biti zamka.
5. Budite oprezni kad od nepoznatog pošiljatelja dobijete e-mail, pogotovo ako sadrži poveznice ili traži od vas osobne podatke, na primjer da potvrdite neku svoju lozinku.
6. Koristite lozinke koje je teško probiti. Redovito ih mijenjajte i nemojte koristiti istu lozinku za više korisničkih računa.
7. Informacije o kreditnim karticama ili svom bankovnom računu ostavljajte samo na provjerenim i zaštićenim web-stranicama.
8. Pazite na to da točno upisujete web-adrese, pogotovo kad je riječ o stranicama financijskih ustanova. Zbog samo jednog pogrešno upisanog slova mogli biste se naći na lažnoj stranici.
9. Kad otkrivete povjerljive informacije, na primjer pojedinosti o svojoj kreditnoj kartici, koristite web-stranice koje omogućuju kodiranje podataka i odjavite se sa stranice nakon što ste je koristili.
10. Redovito pažljivo provjeravajte izvještaje o stanju na bankovnim računima i kreditnim karticama. Čim primijetite neku sumnjivu transakciju, odmah o tome obavijestite banku ili izdavača kreditne kartice.
11. Budite na oprezu kad ste spojeni na Internet putem nezaštićene bežične (Wi-Fi) mreže jer vam napadači mogu ukrasti podatke ili vas preusmjeriti na lažne web-stranice.
12. Ako vas web-preglednik upita želite li da zapamti vašu lozinku, zanemarite taj prijedlog. Trojanski konji lako mogu doći do pohranjenih lozinki.

#### 1.4. Svojevoljno ostavljanje podataka

U ovom poglavlju opisuju se scenariji u kojima korisnici svojevoljno ostavljaju podatke na društvenim mrežama, *loyalty* programima, stranicama za e-trgovinu i sl. te za što se ti podaci mogu koristiti. Pritom se nužno ne događaju prijevare na izravnu štetu korisnika kao one opisane u prošlom poglavlju (gubitak novaca, instalacija virusa), ali korisnici moraju biti svjesni što sve različite usluge na Internetu znaju o njima i na koji to način mogu koristiti.

##### 1.4.1. Društvene mreže

Pri učlanjivanju na društvene mreže korisnici mogu pružiti brojne podatke o sebi. Uglavnom se za otvaranje korisničkih računa traže samo ime, prezime i e-mail adresa. Dodatno, korisnik može ako želi ostaviti i podatke poput adrese, brojeva telefona, zaposlenju, datumu rođenja. Pri svakodnevnom korištenju društvenih mreža, mogu se ostaviti podaci poput trenutne lokacije, planova za budućnost (putovanja i sl.), slike i sl.

Ako te podatke vide drugi korisnici s nečasnim namjerama, mogu izvršiti različite prijevare, poput krađe identiteta (predstavljaju se pod tuđim imenom i prezimenom) i provale u stan (lopovi znaju gdje se koji stanar nalazi ako to objavi na društvenoj mreži). Dodatno, korisnici mogu postati metama za očajnike koji se lažno predstavljaju i traže društvo (*catfishing*). Mogu imati i probleme u poslovnom životu jer poslodavci mogu saznati nešto što će utjecati na njihovu odluku da nekog zaposle (slike nedoličnog ponašanje itd.). Stvari dostupne na društvenim mrežama postaju jedan od čimbenika za procjenu osobnosti pri zapošljavanju, stipendiranju i sl.

Da bi se korisnik zaštitio, mora paziti na postavke privatnosti, ručno odabrati što želi dijeliti i s kime, i ako se nešto dijeli javno, treba biti svjestan da to svatko može vidjeti i spomenuti u bilo kojem trenutku.

##### 1.4.2. *Loyalty* programi

Mnoge kompanije daju *loyalty* kartice kao pogodnost pri kupovini. Moguće je prikupljanje određenog broja bodova radi ostvarivanja popusta. Od korisnika se traže sljedeći podaci za registraciju: e-mail adresa, fizička adresa, ime i prezime, broj telefona, datum rođenja, podatci o kreditnoj kartici.

Ovo je još jedan od načina kako prikupiti osjetljive podatke od korisnika koje uključuju osobne podatke kao i podatke o kupovnim navikama: gdje kupuju, što kupuju i sl.

Opći uvjeti poslovanja uglavnom u ovakvim slučajevima potvrđuju sljedeće: Privatnost je zagarantirana, ali pristankom na korištenje kartice davatelj usluge ima pravo prikupljati podatke o vašim navikama i aktivnostima te zajedno s vašim privatnim podacima dijeliti ih s trećom stranom u svrhu marketinških istraživanja i sl.

Dakle, pri učlanjivanju u *loyalty* programe korisnici moraju biti svjesni da davatelji usluga znaju njihove kupovne navike, ali mogu znati i njihovo kretanje ovisno o tome u kojim dućanima se kupuje, što mogu dijeliti i s nekim drugim tvrtkama. Ti podaci se većinom koriste za dodjeljivanje popusta, preporučivanje proizvoda i sl.

### 1.4.3. *Online* download igara

Kod ovog načina prijevara *online* igre se dobivaju besplatno te se nakon određenog vremena igranja i savladanih nekoliko nivoa traži da se kupi dodatna (energija, vrijeme, oružje, itd.) za daljnji nastavak igre ili prelazak na novi nivo. Od korisnika se traže sljedeći podaci za registraciju: e-mail adresa, fizička adresa, ime i prezime, broj telefona, datum rođenja, podaci o kreditnoj kartici.

Opći uvjeti poslovanja u ovakvim slučajevima uglavnom potvrđuju sljedeće: Privatnost je zagarantirana, ali pristankom na igranje davatelj usluge ima pravo prikupljati podatke o vašim navikama i aktivnostima te vaše privatne podatke dijeliti s trećom stranom u svrhu marketinških istraživanja i sl., te često *software* koji je instaliran prati sve aktivnosti vašeg računala ili pokretnog uređaja.

## 1.5. Kalkulator rizika

Usluge na Internetu danas, s posebnim naglaskom na usluge na pokretnim uređajima (npr. Android ili iOS *smartphone* uređajima), zahtijevaju od korisnika puno privatnih podataka. Razlog tome je kako bi mogle što bolje prilagoditi krajnjem korisniku i pružiti mu personalizirani sadržaj i uslugu, s ciljem pružanja boljeg korisničkog iskustva. Prema direktivi Europske Unije o privatnosti [13], svi osjetljivi korisnički podaci mogu se prikupljati tek nakon eksplicitnog pristanka korisnika i mogu se spremati i obrađivati samo tijekom vremena dok korisnik koristi određenu uslugu.

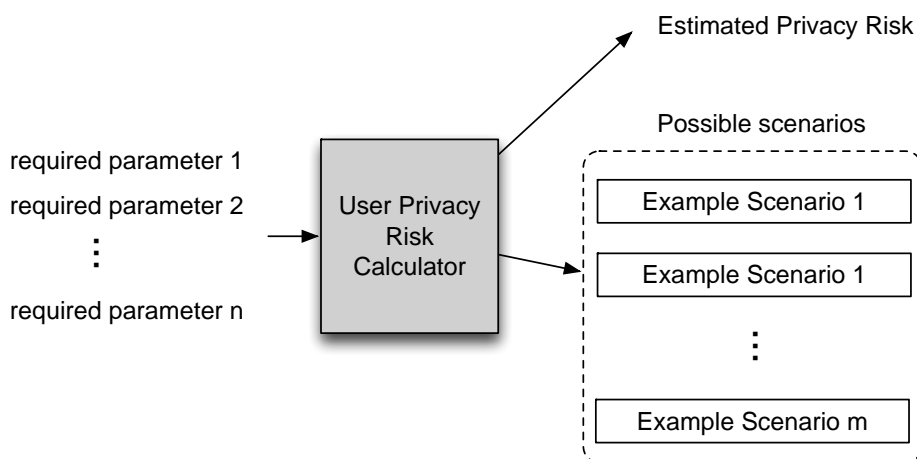
Međutim, glavni problemi s osjetljivim korisničkim podacima pojavljuju se u slučaju ciljane povrede podataka (engl. *data breach*) ili tijekom njihovog dijeljenja između pružatelja usluga. Napadi na podatke najčešće su rezultat loših sigurnosnih karakteristika aplikacija i usluga. Također, napadači puno češće napadaju upravo pružatelje usluga jer na taj način mogu lakše doći do podataka o velikim grupama korisnika. S druge strane, prodaja i razmjena privatnih korisničkih podataka između usluga, najčešće u marketinške svrhe, također je vrlo česta meta napadača koji ukradene osobne podatke najčešće nastoje iskoristiti u različitim prijevarama, o čemu je bilo dosta riječi u prošlim poglavljima.

Glavni problem korisnika najčešće je činjenica da nisu svjesni rizika povrede privatnosti odavanja privatnih podataka te ne razumiju potencijalne posljedice takvog čina. U tom smislu, glavni cilj predloženog kalkulatora rizika povrede privatnosti korisnika je pokušati podići svijest o tim opasnostima među korisnicima web-usluga.

Ideja se temelji na analizi korisničkih podataka koje pojedine usluge zahtijevaju za normalno funkcioniranje. Ti se podaci mogu promatrati kroz popis parametara usluge (npr. ime, prezime, e-mail adresa, itd.). Svaki pojedini parametar uz sebe nosi i određene rizike povrede privatnosti ukoliko bude ukraden i zloupotrijebljen. Nadalje, kombiniranje više parametara zajedno agregira rizike. Cilj je analizirati skupove korisničkih parametara, koje zahtijeva pojedina usluga, i na temelju te analize procijeniti rizik povrede privatnosti vrijednošću između 0 i 1. Ako je rizik procijenjen na 0, to znači da zapravo i nema rizika povrede privatnosti korisnika, a procjena u iznosu od 1 sugerira najveći mogući rizik. Kako bi navedeni rezultati bili razumljiviji krajnjim korisnicima, uz brojčanu vrijednost prikazuje se i

*heatmap* na kojem nijanse zelene boje označavaju male vrijednosti rizika, a crvena boja označava suprotnu situaciju velikog rizika.

Budući da je cilj podići korisničku svijest o problemima privatnosti, samostalna procjena rizika nije dovoljna. Kako bi se korisnicima dao bolji uvid u potencijalne opasnosti, uz svaku procjenu rizika povrede privatnosti dolazi i opis nekoliko scenarija iz svakodnevnog života (slično kao u poglavlju 1.2) do kojih može doći zbog neopreznog rukovanja privatnim podacima.



Slika 5. Koncept kalkulatora za procjenu rizika povrede privatnosti korisnika

Koncept kalkulatora za procjenu rizika povrede privatnosti korisnika prikazan je na Slici 1. Ulazne vrijednosti su korisnički podaci koje zahtijevaju pojedine aplikacije i usluge. Izlazne vrijednosti su procjena rizika praćena opisom nekoliko scenarija iz stvarnog života. Predloženi kalkulator biti će implementiran u obliku web-aplikacije i krajnji korisnici će mu moći jednostavno pristupiti putem svojih web-pretraživača.

Prije korištenja kalkulatora, učitavaju se unaprijed definirani skupovi pravila. Ta pravila definiraju preslikavanje između ulaznih i izlaznih parametara kalkulatora. Pravila se definiraju nakon ljudske analize rizika povrede privatnosti korisnika. Svako pravilo  $R_i$  sastoji se od:

- skupa  $P_i$  od  $n$  privatnih korisničkih parametara  $rp_j$  koje zahtijeva pojedina usluga/aplikacija:

$$P_i = \{rp_1, rp_2 \dots rp_n\}$$

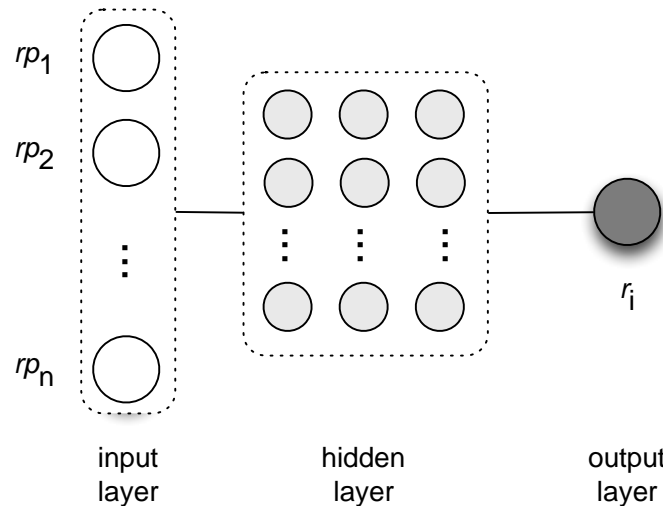
- procjene rizika povrede privatnosti korisnika  $r_i$
- skupa  $S$  koji sadrži  $m$  scenarija  $s_k$  koji odgovaraju ulaznim parametrima:

$$S_i = \{s_1, s_2 \dots s_m\}$$

Kalkulator rizika preslikava ulazne parametre na unaprijed definirane vrijednosti rizika povrede privatnosti korisnika i pripadajuće opise scenarija. Svako pojedino pravilo u tom smislu predstavlja dva zasebna preslikavanja:

$$\begin{aligned} & \text{risk calculation: } P_i \rightarrow r_i \\ & \text{example scenarios: } P_i \rightarrow S_i \end{aligned}$$

Međutim, unaprijed definirani skupovi pravila samo su dio potrebnih kombinacija parametara, stoga postoji potreba za prilagodljivijim i inteligentnijim preslikavanjem. Kako bi se procjene rizika mogle provoditi i za unaprijed nepoznate kombinacije ulaznih parametara, predlaže se korištenje *feedforward* neuronske mreže (engl. *neural network*) prikazane na Slici 2.



Slika 6. Neuronska mreža za procjenu rizika povrede privatnosti korisnika

Neuronska mreža sastoji se od  $n$  ulaznih neurona koji odgovaraju potrebnim ulaznim parametrima koje koriste usluge. Prisutnost pojedinog parametra na ulazu naznačena je aktivacijom neurona s vrijednošću 1, dok odsutnost parametra rezultira u aktivaciji vrijednosti 0. Izlazni sloj sastoji se od neurona čija aktivacija odgovara procjeni rizika povrede privatnosti korisnika (između 0 i 1). Skriveni sloj sadrži nekoliko neurona i njegova se veličina određuje eksperimentalno.

Neuronska mreža trenira se pomoću poznatih pravila i preslikavanja prilikom procjene rizika povrede privatnosti. Pretpostavka je da skup za učenje ne pokriva sve moguće kombinacije ulaznih parametara. Stoga, kako mreža uči sposobna je vršiti precizne procjene rizika povrede privatnosti korisnika sukladno vrijednostima u skupu za učenje. Prema tome, glavna prednost predložene arhitekture je što je kalkulator ipak sposoban vršiti procjene rizika u slučaju pojave novih, do tada nepoznatih kombinacija parametara na ulazu.

Iako se predložena neuronska mreža može vrlo dobro nositi s procjenom rizika, ovakvo rješenje nije prilagodljivo i u slučaju primjera opisnih scenarija. Razlog tome je činjenica da su scenariji znatno kompleksniji te se moraju prikazati u ljudima razumljivom obliku. Prema tome, kalkulator će na pojavu nove kombinacije ulaznih parametara uspješno izvršiti procjenu rizika povrede privatnosti korisnika, međutim neće samostalno generirati opis scenarija iz svakodnevnog života. Jedna od mogućnosti rješenja ovog nedostatka davanje je najbližeg postojećeg scenarija kao predloženog rezultata.

## 1.6. Zaključak

Privatnost korisnika postaje problem na Internetu zbog sve češćih povreda podataka i sigurnosnih prijetnji. Osim ograničenja tehničkih metoda za zaštitu korisničkih privatnih podataka, glavni problem je niska razina svijesti korisnika o mogućim prijevarama i sličnim kaznenim djelima putem Interneta.

Cilj ovog rada je razviti kalkulator koji na temelju ulaznih parametara koje zahtijevaju različite web-usluge pokušava procijeniti mogući rizik povrede privatnosti korisnika, ako su ti podaci procurili ili ih napadač nastoji zloupotrijebiti na bilo koji način. Uz procjenu rizika, kalkulator daje i opise najčešćih prijevara. Predstavljajući česte prijevare u čitljivom i na ljudima razumljiv način, doprinosi razvoju veće svijesti korisnika o potencijalnim rizicima povrede privatnosti.

Buduća istraživanja će biti usmjerena na širenje baze prijevara i njena integracija u kalkulator rizika. Osim toga, usredotočiti ćemo se na razvoj dodatne programske logike koja će biti u mogućnosti bolje obraditi nove kombinacije ulaznih parametara koji mogu biti potrebni u budućnosti, pogotovo u kontekstu aplikacija i usluga za pokretne uređaje.



## 1.7. Literatura

- [1] Phishing Scams - Anti-Phishing Information, <http://www.hoax-slayer.com/phisher-scams.html>, pristupljeno 15.6.2014.
- [2] Advance Fee Scams - Nigerian Scams - 419 Scam Information, <http://www.hoax-slayer.com/nigerian-scams.html>, pristupljeno 15.6.2014.
- [3] Payment Transfer Job Scams - Laundering Scams, <http://www.hoax-slayer.com/money-transfer-job-scams.shtml>, pristupljeno 15.6.2014.
- [4] Pharming - Information about Pharming Scams, <http://www.hoax-slayer.com/pharming.html>, pristupljeno 15.6.2014.
- [5] Internet Dating Scams, <http://www.hoax-slayer.com/internet-dating-scams.shtml>, pristupljeno 16.6.2014.
- [6] Advance Fee Lottery Scams - International Lottery Scam Information, <http://www.hoax-slayer.com/email-lottery-scams.html>, pristupljeno 16.6.2014.
- [7] Scams on social networks that will surprise you, <http://support.pandasecurity.com/blog/security/scams-social-networks-will-surprise/>, pristupljeno 16.6.2014.
- [8] Facebook Pyramid Investment Scheme Busted, <http://facecrooks.com/Scam-Watch/Facebook-Pyramid-Investment-Scheme-Busted.html/>, pristupljeno 16.6.2014.
- [9] Beware of Bogus UGG Outlet Store Scams on Facebook, <http://facecrooks.com/Scam-Watch/Beware-Bogus-UGG-Outlet-Store-Scams-Facebook.html/>, pristupljeno 16.6.2014.
- [10] [Phishing Alert] Facebook Scam Says Users' Friends Have Been the Victim of Crime, <http://facecrooks.com/Scam-Watch/Phishing-Alert-Facebook-Spam-Says-Users-Friends-Have-Been-Victim-Crime.html/>, pristupljeno 16.6.2014.
- [11] Beware of iPhone Giveaway Scams on Facebook, <http://facecrooks.com/Scam-Watch/Beware-iPhone-Giveaway-Scams-on-Facebook.html/>, pristupljeno 16.6.2014.
- [12] New Facebook Malware Suggests Phony "Pages You Might Like", <http://facecrooks.com/Scam-Watch/New-Facebook-Malware-Suggests-Phony-Pages-You-Might-Like.html/>, pristupljeno 16.6.2014.
- [13] Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on Privacy and Electronic Communications), *European Parliament and Council*, 2002.

### 3. Evaluacija kalkulatora za procjenu rizika povrede privatnosti korisnika

#### 3.1. Uvod

Privatnost korisnika na Internetu je zbog sve češćih povreda privatnosti i sigurnosnih prijetnji postala predmet analiza znanstvenika i sigurnosnih stručnjaka. Usluge danas zahtijevaju privatne korisničke podatke kako bi pružile što bolju personaliziranu uslugu, no većina njihovih korisnika nije svjesna potencijalnih prijetnji koje iz toga proizlaze. Ovaj rad predlaže kalkulator rizika zasnovan na „feedforward“ neuronskoj mreži koji će korisnicima omogućiti izračun rizika povrede privatnosti. Osim toga, kako bi se pružio bolji uvid u razumijevanje problema privatnosti, svaki od rizika dodatno će biti razjašnjen pomoću nekoliko stvarnih scenarija koji se mogu dogoditi ukoliko napadač dođe u posjed privatnih korisničkih podataka. Sve navedeno trebalo bi podići svijest i znanje korisnika o potencijalnim problemima privatnosti na Interneta, te potaknuti široku javnu raspravu svih zainteresiranih strana u svrhu pronalaska boljeg regulatornog okvira za rješavanje navedenih problema.

Povreda privatnosti korisnika na Internetu u današnjem je društvu postala ozbiljan i široko rašireni problem. Usluge poput društvenih mreža i *online* trgovina traže od korisnika niz privatnih podataka bez kojih ne mogu normalno funkcionirati. Pružatelji usluga na taj način raspolazu golemom količinom vrlo osobnih informacija o korisnicima koje je vrlo lagano zloupotrebjavati. Dodatan problem je činjenica da korisnici nisu svjesni potencijalnih rizika i posljedica takvih zlonamjernih aktivnosti. Unatoč tome, korisnici i dalje u velikom broju i vrlo lako prihvaćaju nove usluge, a vrlo rijetki korisnici s vremenom odbijaju korištenje tih usluga zbog potencijalnih problema vezanih uz njihove privatne podatke.

S obzirom na veliku odgovornost, pružatelji personaliziranih usluga trebaju imati pripremljene adekvatne sigurnosne mjere kako bi zaštitili privatne podatke korisnika od potencijalnih zlonamjernih aktivnosti. Posebno je važno za korisnike da ih njihov pružatelj usluga transparentno obavijesti o postojećim sigurnosnim opasnostima koje leže izvan opsega mogućih sredstava za otklanjanje opasnosti koje on može pružiti.

Ovaj izvještaj nastavak je suradnje FER-a i HAKOM-a čiji je krajnji cilj korisnike upoznati s mogućim opasnostima te potaknuti stručnu javnost za potrebe novih pogleda i stvaranja novih regulatornih okvira privatnosti na Internetu.

U poglavlju 1.2 dan je pregled srodnih istraživanja u području povreda privatnosti, a poglavlje 1.3 donosi opis i model kalkulatora zasnovanog na neuronskim mrežama koji procjenjuje rizik povrede privatnosti korisnika. Evaluacija predloženog kalkulatora dana je u poglavlju 1.4, dok se u poglavlju 1.5 iznose zaključci, kao i osvrt na buduća istraživanja.

### 3.2. Srodna istraživanja

Kada se govori o različitim napadima na privatnost korisnika, internetskim prijevarama (engl. *scams*) ili zlonamjernim „cyber“ aktivnostima u cjelini, teško ih je sve ujediniti pod jednim zajedničkim pojmom. Ti napadi mogu uključivati krađu pristupa bankovnom računu ili kreditnoj kartici, oduzimanje intelektualnog vlasništva, izradu i distribuciju zlonamjernog (engl. *malware*) softvera (primjerice, „trojanskih konja“, *adware* ili *spyware* programa) na druga računala ili zaustavljanje rada kritične nacionalne infrastrukture poput električne mreže u nekoj zemlji. Također, teško je povući jasnu crtu između svake od tih pojedinačnih aktivnosti. Poruke neželjene elektroničke pošte (engl. *spam*) mogu oglašavati neki dosadni i nepotrebni proizvod, ali isto tako mogu poslužiti i kao transportni medij za sofisticirani zlonamjerni kod. Jedina veza svih navedenih zlonamjernih i potencijalno kriminalnih aktivnosti je činjenica da se provode putem Interneta [1]. Prema Internet World Stats [2], na kraju 2012. godine više od 2,4 milijarde ljudi koristilo se Internetom. Takva velika *online* populacija otvara puno prilika zlonamjernim korisnicima i kriminalcima, a financijska šteta koja je posljedica njihovih zlonamjernih aktivnosti mjeri se u stotinama milijuna ili čak milijardama dolara svake godine. Razne provedene studije iznose različite procjene, ovisno o tome koje su aktivnosti promatrane te kako je njihov utjecaj vrednovan i uključen u krajnji izračun cijene štete. McAfee Centar za strateške i međunarodne studije svake godine objavljuje studiju o ekonomskom utjecaju kriminala izvršenog posredstvom Interneta, a brojevi za 2013. godinu [3] su sljedeći: ukupna šteta u SAD-u procjenjuje se na iznos između 24 i 120 milijardi dolara (između 0,2 % i 0,8 % BDP-a SAD-a), dok se u svijetu taj iznos kreće od 300 milijardi do 1 bilijuna dolara (od 0,4 % do 1,4 % ukupnog svjetskog BDP-a). Druga studija [1], usmjerena na analizu stanja u 234 tvrtke u 6 zemalja (SAD, Velika Britanija, Njemačka, Australija, Japan i Francuska), procjenjuje vrijednost financijske štete u pojedinoj tvrtci između 3,67 milijuna dolara u prosjeku za Australiju do 11,56 milijuna dolara u SAD-u. Istraživanje o krađi identiteta provedeno na Sveučilištu Cambridge procjenjuje neto trošak od krađe identiteta za pojedinu žrtvu u iznosu od 572 dolara [4]. Kao posljedica toga, neki od znanstvenih napora u ovom području usmjereni su na razvoj efikasnijih sredstava za zaštitu korisnika od *phishing* napada [5][6]. Takve i slične studije o troškovima zlonamjernih *online* aktivnosti obično su predmet kritika jer vrlo često ne razgraničavaju jasno utjecaj na nacionalnu sigurnost, utjecaj na poslovanje tvrtke što dovodi do gubitaka i pada povjerenja potrošača, i na kraju štetni utjecaj na pojedine korisnike Interneta. Međutim, sve studije na kraju dovode do istog zaključka, a to je da zlonamjerne kriminalne aktivnosti provedene preko Interneta u bilo kojem obliku uzrokuju potencijalno velike financijske troškove i iz godine u godinu sve više rastu. Sve navedeno je dovelo do povećanih napora kako bi se popisalo, opisalo (npr. [7][8]), otkrilo (npr. [9][10]) i na kraju izmjerilo prijetnje na Internetu.

Uloga prijetnji u procjeni rizika vezanih za informacijsku sigurnost opisana je u dokumentu ISO/IEC 27005:2011 [10]. Ovaj vodič opisuje opće pojmove navedene u ISO/IEC 27001:2013 [10], osmišljen je kako bi se pomoglo pri zadovoljavajućoj uspostavi sigurnosti informacijskih sustava koji se temelji na pristupu upravljanja rizikom, a odnosi se na sve vrste organizacija (komercijalna poduzeća, vladine agencije, neprofitne organizacije, itd.). Rizici, prema definiciji, nastaju kada „prijetnje iskorištavaju ranjivosti imovine s ciljem generiranja

štete za organizaciju“. Analizirajući malo detaljnije, rizik se razmatra kada se uzmu u obzir sljedeći elementi i njihova međuovisnost:

- sredstva (ranjivosti (engl. *Vulnerabilities*), kontrole (engl. *Controls*)),
- prijetnja (profil napadača (engl. *Threat Agent Profile*), vjerojatnost (engl. *Likelihood*)),
- utjecaj (engl. *Impact*).

Napadači (engl. *Threat Agents*, TA) izvršavaju prijetnje (engl. *Threats*, T) s ciljem iskorištavanja ranjivosti (engl. *Vulnerabilities*, V) resursa/imovine (engl. *asset*). Imovina mora imati postavljene sigurnosne mjere (engl. *Measures*, M) kako bi se zaštitila, tj. kako bi se uklonili negativni učinci od izloženosti prijetnji. Završni element jednadžbe za procjenu rizika imovine je potencijalna materijalizacija prijetnje. Iako je ovo općeniti scenarij definiran u kontekstu upravljanja rizicima, sličan se scenarij može ispitati i u malo širem kontekstu. Općenito, puno je lakše nabrojati prijetnje, nego ih opisati, posebno u složenim okruženjima zbog različitih sposobnosti imovine, njihovih mogućih ranjivosti i sigurnosnih propusta, te sposobnosti napadača i njima dostupnih metoda napada. Sljedeći korak, mjerenje prijetnji, još je teže ostvariti. Kao rezultat toga, mnoge su organizacije sposobne nabrojati prijetnje, ali puno manji broj njih su sposobne opisati ih i još manji broj je u mogućnosti izmjeriti ih na smislen način [13].

Sposobnost mjerenja prijetnji donosi nekoliko prednosti. Primjerice, kvalitetno mjerenje prijetnji može olakšati analizu, pokazati trendove i anomalije, otkriti specifične ranjivosti, te pomoći pri identificiranju potencijalnih posljedica prijetnji. Drugim riječima, dobro mjerenje prijetnji omogućuje dobro upravljanje rizicima. U posljednjih nekoliko godina razvijeno je nekoliko kalkulatora „rizika“ i „prijetnji“ koji mogu izračunati ili procijeniti potencijalni rizik povezan s određenom *online* prijevaram ili prijetnjom. Takve tehnike su postale popularne u poslovnoj domeni jer tvrtke na taj način mogu odrediti barem kvalitativnu i/ili kvantitativnu razinu prijetnji i s njima povezanih rizika. Dakle, ti kalkulatori koriste prikupljene podatke kao pomoć pri donošenju boljih odluka, ovisno o datoj situaciji odlučuju koje je sigurnosne mjere potrebno poduzeti te na taj način sugeriraju u koje se sigurnosne tehnologije i strategije doista isplati ulagati. Jedan od primjera je kalkulator Prolexic DDoS (engl. *Distributed Denial-of-Service*) [14] koji izračunava utjecaj raspodijeljenog napada uskraćivanja usluge na dostupnost web-stranice. DDoS napadi različito utječu na različite tvrtke: što može izazvati ozbiljan zastoj kod jedne web-stranice, može imati minimalan utjecaj na druge. Kalkulator se temelji na nizu dubinskih pitanja, na kraju daje rezultate koji odražavaju jedinstveno sigurnosno i mrežno okruženje pojedine tvrtke, a također pruža i savjete. Drugi primjer kalkulatora temeljenog na upitniku je Symantec Cyber Resilience Assessment [16] koji pruža personaliziranu procjenu sigurnosnih procedura za pojedinu organizaciju, pomaže pri identifikaciji potencijalnih slabosti i preporučuje najbolje strategije i rješenja za njihovo uklanjanje. Symantec je također razvio niz mjerila za procjenu prijetnji [17] koje se fokusiraju na različite aspekte sigurnosti sustava. Prvo mjerilo analizira širenje zlonamjernog koda i potencijalne štete koje može prouzročiti, te predlaže mjere ovisno o izračunatoj kategoriji prijetnje. Definira ukupno pet kategorija rizika za korisnike: Kategorija 1 (Cat 1) označava

najmanju razinu prijetnji, a Kategorija 5 (Cat 5) najveću. Drugo mjerilo bavi se zlonamjernih aktivnostima, od bezopasnih HTTP (engl. *Hypertext Transfer Protocol*) skeniranja do pravih napada na privatne mreže, uz prioritiziranje odgovora na napad temeljem relativne razine opasnosti. Svaka aktivnost svrstava se u jednu od četiri kategorije: obavijesna, upozorenje, kritična i hitna. Treća Symantecova metrika kategorizira ranjivosti sustava u sljedeće razine: niska (0-3), umjerena (4-7) i visoka (8-10). Razina ranjivosti temelji se na nekoliko kriterija: relativnom utjecaju na sustav, daljinskoj iskoristivosti, zahtjevu za provjerom identiteta i dostupnosti sustava zahvaćenog napadom. Primjer kalkulatora za procjenu rizika razvila je i tvrtka ParadosLabs [18], a koji se bazira na metodologiji za ocjenu rizika OWASP (*Open Web Application Security Project*) [19]. Uključuje informacije o napadaču, vrsti prijetnje koja će se koristiti, pridruženim ranjivostima i razini utjecaja uspješne prijetnje na posao. Čimbenici zasnovani na prve dvije kategorije (napadač i ranjivosti) pomažu odrediti razinu vjerojatnosti prijetnje, dok čimbenici zasnovani na posljednje dvije kategorije (tehnički i poslovni utjecaj) pomažu odrediti razinu utjecaja prijetnje. Na temelju ta dva izvedena parametra određuje se ukupna razina rizika ozbiljnosti prijetnje: vrlo niska, niska, srednja, visoka ili izrazito visoka. Istraživački tim Sveučilišta u New Hampshireu razvio je 2007. godine kalkulator za procjenu rizika koje razni entiteti predstavljaju preko Interneta za nacionalnu infrastrukturu SAD-a [20]. Kalkulator na temelju unesenih podataka za određene organizacije ili zemlje mjeri njihovu potencijalnu namjeru i tehnološke mogućnosti za provedbu napada preko Interneta na američku infrastrukturu. Sličan projekt proveden je od strane tima izraelskih stručnjaka, koji su kao rezultat predložili indeks osjetljivosti od napada izvršenih preko Interneta (engl. *Cyber-Attack Susceptibility, CAS*). Indeks se koristi za procjenu u kakvom su stanju pojedine zemlje nositi se s potencijalnim napadima preko Interneta na njihovu kritičnu infrastrukturu [21].

Svi ranije navedeni primjeri tiču se ili zlonamjernih aktivnosti vezanih uz poslovanje poduzeća ili napade na državnu infrastrukturu i/ili njezine agencije. Štoviše, većina financijskih studija, od kojih su neke navedene na početku ovog poglavlja, prvenstveno su usredotočene na te dvije „razine“ korisnika Interneta, a svega nekoliko njih stavlja naglasak na pojedine korisnike Interneta. *Online* prijetnje u obliku neželjene elektroničke pošte (engl. *spam*), *phishinga* i nigerijskih prijevara (engl. *nigerian scams*) putem e-maila ili društvenih mreža dokazale su da mogu imati ozbiljne posljedice, od krađe pristupa bankovnom računu ili krađe identiteta do čak otmica ili smrti. Također, tvrtke i državne agencije obično imaju razvijene sustave odgovora na incidente (engl. *Incident Response System*), pripremljene mjere i protumjere te znatno ulažu u najnovija hardverska i softverska rješenja. Također, svojim radnicima osiguravaju odgovarajuću razinu obrazovanja i osposobljavanja u domeni sigurnosti na Internetu. Rezultati istraživanja provedenog u 2007. godini pokazali su razinu spremnosti odgovora na *phishing* napade u bankama iz Hong Konga i Singapura, zajedno s analizom mjera koje se najčešće i najučinkovitije primjenjuju za zaštitu protiv njihovih loših posljedica [22]. Iako individualni korisnici Interneta ako se žele samostalno educirati imaju puno dostupnog materijala po pitanju sigurnog ophođenja na Internetu *online*, smatramo da se na području obrazovanja korisnika i podizanja svijesti može puno više učiniti. Konačno, čini se da niti jedan od do sada razvijenih kalkulatora rizika i razine prijetnji nije široko upotrebljiv u slučaju pojedinačnih korisnika Interneta, a definitivno niti jedan nije prilagođen

hrvatskim korisnicima Interneta. Ovaj projekt je u skladu s dva od četiri programska načela ENISA-e (Agencija Europske unije za mrežnu i informacijsku sigurnost), a to su aktivno uključivanje krajnjih korisnika u obrani od zlonamjernih aktivnosti putem Interneta i povećanje njihovog znanja o *online* prijetnjama [23]. U današnjem vremenu, kada zlonamjerni napadači povećavaju sofisticiranost njihovih napada i prijetnji te se postupno šire na nova područja internetske komunikacije (pokretne mreže i Internet stvari (engl. *Internet of Things*)), ti ciljevi postaju jedni od najvažnijih aktualnih obrazovnih i regulacijskih izazova.

### 3.3. Kalkulator rizika

Usluge na Internetu danas, s posebnim naglaskom na usluge na pokretnim uređajima (npr. Android ili iOS *smartphone* uređajima), zahtijevaju od korisnika puno privatnih podataka. Razlog tome je kako bi se mogle što bolje prilagoditi krajnjem korisniku i pružiti mu personalizirani sadržaj i uslugu, s ciljem pružanja boljeg korisničkog iskustva. Prema direktivi Europske Unije o privatnosti [13], svi osjetljivi korisnički podaci mogu se prikupljati tek nakon eksplicitnog pristanka korisnika i mogu se spremati i obrađivati samo tijekom vremena dok korisnik koristi određenu uslugu.

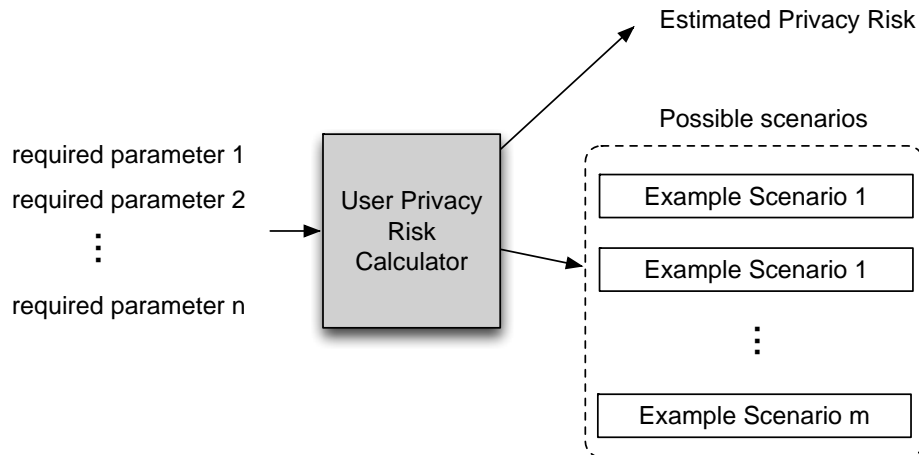
Međutim, glavni problemi s osjetljivim korisničkim podacima pojavljuju se u slučaju ciljane povrede podataka (engl. *data breach*) ili tijekom njihovog dijeljenja između pružatelja usluga. Napadi na podatke najčešće su rezultat loših sigurnosnih karakteristika aplikacija i usluga. Također, napadači puno češće napadaju pružatelje usluga jer na taj način mogu lakše doći do podataka o velikim grupama korisnika. S druge strane, prodaja i razmjena privatnih korisničkih podataka između usluga, najčešće u marketinške svrhe, također je vrlo česta meta napadača koji ukradene osobne podatke najčešće nastoje iskoristiti u različitim prijevarama, o čemu je bilo dosta riječi u prošlim poglavljima.

Glavni problem korisnika najčešće je činjenica da nisu svjesni rizika povrede privatnosti odavanja privatnih podataka te ne razumiju potencijalne posljedice takvog čina. U tom smislu, glavni cilj predloženog kalkulatora rizika povrede privatnosti korisnika pokušati je podići svijest o tim opasnostima među korisnicima web-usluga.

Ideja se temelji na analizi korisničkih podataka koje pojedine usluge zahtijevaju za normalno funkcioniranje. Ti se podaci mogu promatrati kroz popis parametara usluge (npr. ime, prezime, e-mail adresa, itd.). Svaki pojedini parametar uz sebe nosi i određene rizike povrede privatnosti ukoliko bude ukraden i zloupotrebljen. Nadalje, kombiniranje više parametara zajedno agregira rizike. Cilj je analizirati skupove korisničkih parametara, koje zahtijeva pojedina usluga, i na temelju te analize procijeniti rizik povrede privatnosti vrijednošću između 0 i 1. Ako je rizik procijenjen na 0, to znači da zapravo i nema rizika povrede privatnosti korisnika, a procjena u iznosu od 1 sugerira najveći mogući rizik. Kako bi navedeni rezultati bili razumljiviji krajnjim korisnicima, uz brojčanu vrijednost prikazuje se i *heatmap* na kojem nijanse zelene boje označavaju male vrijednosti rizika, a crvena boja označava suprotnu situaciju velikog rizika.

Budući da je cilj podići korisničku svijest o problemima privatnosti, samostalna procjena rizika nije dovoljna. Kako bi se korisnicima dao bolji uvid u potencijalne opasnosti, uz svaku

procjenu rizika povrede privatnosti dolazi i opis nekoliko scenarija iz svakodnevnog života (slično kao u poglavlju 1.2) do kojih može doći zbog neopreznog rukovanja privatnim podacima.



**Slika 1.7.** Model kalkulatora za procjenu rizika povrede privatnosti korisnika

Model kalkulatora za procjenu rizika povrede privatnosti korisnika prikazan je na Slici 1.1. Ulazne vrijednosti su korisnički podaci koje zahtijevaju pojedine aplikacije i usluge. Izlazne vrijednosti su procjena rizika praćena opisom nekoliko scenarija iz stvarnog života. Predloženi kalkulator biti će implementiran u obliku web-aplikacije i krajnji korisnici će moći jednostavno pristupiti putem svojih web-pretraživača.

Prije korištenja kalkulatora, učitavaju se unaprijed definirani skupovi pravila. Ta pravila definiraju preslikavanje između ulaznih i izlaznih parametara kalkulatora. Pravila se definiraju nakon ljudske analize rizika povrede privatnosti korisnika. Svako pravilo  $R_i$  sastoji se od:

- skupa  $P_i$  od  $n$  privatnih korisničkih parametara  $rp_j$  koje zahtijeva pojedina usluga/aplikacija:

$$P_i = \{rp_1, rp_2 \dots rp_n\}$$

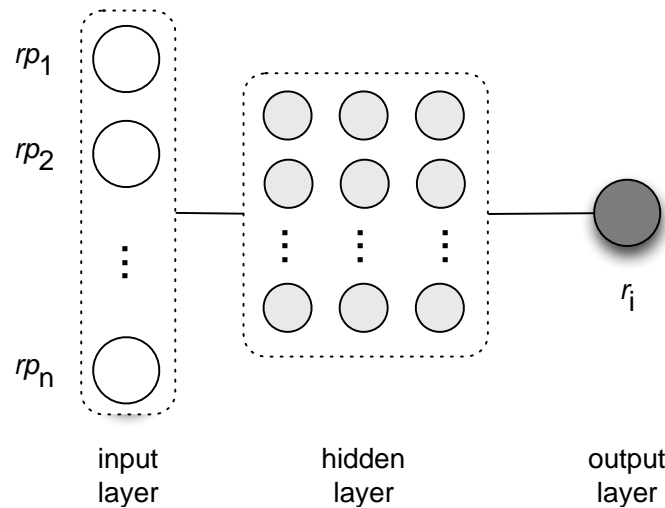
- procjene rizika povrede privatnosti korisnika  $r_i$
- skupa  $S$  koji sadrži  $m$  scenarija  $s_k$  koji odgovaraju ulaznim parametrima:

$$S_i = \{s_1, s_2 \dots s_m\}$$

Kalkulator rizika preslikava ulazne parametre na unaprijed definirane vrijednosti rizika povrede privatnosti korisnika i pripadajuće opise scenarija. Svako pojedino pravilo u tom smislu predstavlja dva zasebna preslikavanja:

$$\begin{aligned} & \text{risk calculation: } P_i \rightarrow r_i \\ & \text{example scenarios: } P_i \rightarrow S_i \end{aligned}$$

Međutim, unaprijed definirani skupovi pravila samo su dio potrebnih kombinacija parametara, stoga postoji potreba za prilagodljivijim i inteligentnijim preslikavanjem. Kako bi se procjene rizika mogle provoditi i za unaprijed nepoznate kombinacije ulaznih parametara, predlaže se korištenje *feedforward* neuronske mreže (engl. *neural network*) prikazane na Slici 1.2.



**Slika 1.8.** Neuronska mreža za procjenu rizika povrede privatnosti korisnika

Neuronska mreža sastoji se od  $n$  ulaznih neurona koji odgovaraju potrebnim ulaznim parametrima koje koriste usluge. Prisutnost pojedinog parametra na ulazu naznačena je aktivacijom neurona s vrijednošću 1, dok odsutnost parametra rezultira aktivacijom vrijednosti 0. Izlazni sloj sastoji se od neurona čija aktivacija odgovara procjeni rizika povrede privatnosti korisnika (između 0 i 1). Skriveni sloj sadrži nekoliko neurona i njegova se veličina određuje eksperimentalno.

Neuronska mreža trenira se pomoću poznatih pravila i preslikavanja prilikom procjene rizika povrede privatnosti. Pretpostavka je da skup za učenje ne pokriva sve moguće kombinacije ulaznih parametara. Stoga, kako mreža uči sposobna je vršiti precizne procjene rizika povrede privatnosti korisnika sukladno vrijednostima u skupu za učenje. Prema tome, glavna prednost predložene arhitekture je što je kalkulator ipak sposoban vršiti procjene rizika u slučaju pojave novih, do tada nepoznatih kombinacija parametara na ulazu.

Iako se predložena neuronska mreža može vrlo dobro nositi s procjenom rizika, ovakvo rješenje nije prilagodljivo i u slučaju primjera opisnih scenarija. Razlog tome je činjenica da su scenariji znatno kompleksniji te se moraju prikazati u ljudima razumljivom obliku. Prema tome, kalkulator će na pojavu nove kombinacije ulaznih parametara uspješno izvršiti procjenu rizika povrede privatnosti korisnika, međutim neće samostalno generirati opis scenarija iz svakodnevnog života. Jedna od mogućnosti rješenja ovog nedostatka davanje je najbližeg postojećeg scenarija kao predloženog rezultata.



### 3.4. Evaluacija

U ovom poglavlju iznose se rezultati evaluacije modela kalkulatora i objašnjavaju odabrani stvarnovremenski scenariji.

Mnoge usluge i aplikacije (npr. društvene mreže, *online* trgovine, programi vjernosti (engl. *loyalty programmes*), itd.) zahtijevaju od korisnika stvaranje osobnog računa uz otkrivanje podataka poput e-mail adrese, imena i prezimena. Ako ti podaci na bilo koji način procure do napadača, on ih može iskoristiti za različite prijevare te na taj način oštetiti korisnika. Slični problemi nastaju kada korisnik odluči omogućiti javnosti pristup svom profilu na društvenoj mreži. Svatko mu može pristupiti i pokušati ga prevariti. Stoga nije nimalo čudno da bi korisnici trebali obratiti posebnu pozornost gdje i kada koriste privatne podatke o primjerice kreditnoj kartici. Međutim, u tom konkretnom slučaju svijest o potrebi pažljivog „dijeljenja“ privatnih podataka na dosta je visokoj razini, za razliku od drugih, naizgled bezazlenijih podataka koji također mogu dovesti do financijskih prijevara, lažnih predstavljanja i drugih prijevara usmjerenih ka korisnicima ili trećim osobama.

Predložena neuronska mreža je trenirana s 20 uzoraka, koji predstavljaju kombinaciju stvarnovremenskih parametara dobivenih iz različitih internetskih usluga (primjerice, Google Mail, Paypal i sl.). Među ulazne parametre se ubrajaju: ime i prezime, spol, datum rođenja, zemlja, broj mobitela, adresa, je li profil korisnika društvene mreže javno dostupan te podaci o kreditnoj kartici. Svakom uzorku ulaznih parametara na izlazu se dodjeljuje vrijednost koja predstavlja procjenu rizika. Izlazne vrijednosti u fazi treningu postavljene su na 0.33, 0.66 i 0.99 što predstavlja nisku, srednju i visoku razinu rizika povrede privatnosti. Tumačenje značenja tih izlaznih vrijednosti je sljedeće:

- niska razina rizika (0.33 i niže) ne predstavlja izravnu opasnost za korisnike; Napadač može pokušati iskoristiti privatne podatke za prijevaru korisnika ili treće osobe s neizvjesnim ishodom.
- srednja razina rizika(0.34-0.66) daje napadaču mogućnost iskorištavanja privatnih korisničkih podataka u pokušaju prijave korisnika ili treće osobe, uz višu razinu uspjeha; ciljano sudjelovanje korisnika može biti potrebno.
- visoka razina rizika (0.67-0.99) ukazuje na to da napadač može napraviti znatnu štetu korisniku ili trećim osobama, bez potrebe za daljnjim obmanjivanjem korisnika ili zahtjevom za njegovim dodatnim sudjelovanjem.

Rezultati provedene evaluacije za odabrane uzorke ulaznih parametara prikazani su u Tablici 1.1. Tablica prikazuje parametre koji su sadržani u ulaznom uzorku te procjene rizika na izlazu mreže. Svakom uzorku (retku u tablici) dodjeljuje se scenarij, dok stupac „Treniran“ pokazuje je li uzorak bio uključen u fazu treninga neuronske mreže.

**Tablica 1.1.** Evaluacija odabranih uzoraka ulaznih parametara neuronske mreže

Rb Sc.	Korisnički parametri	Treniran	Procjena razine rizika
S1	ime, spol, datum rođenja, zemlja	Da	0.33 niska
S2	e-mail adresa, ime, spol, datum rođenja, adresa	Da	0.66 srednja
S3	ime, spol, datum rođenja, zemlja, broj mobitela (podaci za uslugu Gmail)	Da	0.66 srednja
S4	e-mail adresa, ime, spol, datum rođenja, adresa, broj kreditne kartice (podaci za uslugu PayPal)	Da	0.99 visoka
S5	e-mail adresa	Ne	0.43 srednja
S6	ime, broj mobitela	Ne	0.62 srednja
S7	javni profil društvene mreže	Ne	0.64 srednja
S8	ime, broj kreditne kartice	Ne	0.98 visoka

Scenarij S1 predstavlja slučaj u kojem korisnik daje njegove/njezine opće podatke. Odgovarajući uzorak je bio uključen u fazu treninga i razina rizika je postavljena na 0.33, što je isto kao i izlaz neuronske mreže, kako se i očekivalo (srednja kvadratna pogreška nakon treninga bila je manja od  $1 \times 10^{-4}$ ). Iako ovaj slučaj može predstavljati situaciju prijatnje, smatra se da je njena razina niska, jer je većina tih podataka vrlo lako dobavljiva i ne sadrži podatke za kontakt korisnika što bi napadač mogao iskoristiti u pokušaju njegova zavaravanja.

Scenarij S2 je sličan S1, ali sadrži e-mail adresu i adresu stanovanja korisnika pa je napadač sada u mogućnosti izravno kontaktirati korisnika. Poznavanje e-mail adrese se obično koristi za zavaravanje korisnika ili lažno predstavljanje u ime korisnika prema trećim osobama. Osim primanja neželjenih poruka elektroničke pošte, primjeri prijevara koje se mogu realizirati zloupotrebom e-mail adrese uključuju nigerijsku prijevaru i njene varijacije [25], kao i *phishing* napade. Nadalje, adresa stanovanja može se koristiti za kontaktiranje korisnika uživo, čime se otvara novi spektar mogućnosti za obmanu korisnika.

Scenarij S3 sadrži parametre potrebne prilikom registracije na uslugu Gmail, što je preduvjet za razne usluge i aplikacije koje nudi Google. Parametar broj mobitela je potreban za

poboljšanu autentifikaciju korisnika. Međutim, ako napadač, zajedno s drugim parametrima, ukrade korisniku broj mobitela, to otvara novi spektar mogućih prijevara, vrlo sličnima onima iz scenarija S2. Primjerice, zlonamjerni napadač može natjerati korisnika na zvanje specifičnog broja telefona, što u konačnici rezultira visokim financijskim troškovima. Sličan primjer u praksi nedavno je primjećen u Hrvatskoj, u kojem korisnik dobiva SMS poruku koja zahtijeva hitan poziv. Pozvani broj je zapravo usluga na dodanu vrijednost (engl. *value added service*) registrirana u jednoj od afričkih zemalja i zvanje se pokazalo iznimno skupom „avanturom“ za korisnike koji su nasjeli na prijevaru.

Prethodni scenariji su zahtijevali akciju korisnika kako bi se prijevara provela u djelo i stoga su označeni s niskom ili srednjom razinom rizika. Međutim, scenarij S4 sadrži podatke o kreditnoj kartici korisnika, koje napadač može iskoristiti bez intervencije korisnika. U stvarnosti to znači otprilike sljedeće: korisnici za kupnju proizvoda iz *online* trgovine koriste kreditnu karticu, a *online* trgovina brojeve kreditnih kartica pohranjuje u zapisnicima poslužitelja ili slično (nenamjerno). Napadači se fokusiraju na te poslužitelje i pokušavaju izvući povjerljive podatke. Nažalost, korisnici nisu u mogućnosti spriječiti ove vrste napada, već njihova sigurnost ovisi o kvaliteti sigurnosne infrastrukture *online* trgovine. Najčešći oblik ranjivosti povezan s kreditnim karticama je ako njihovi brojevi nisu dovoljno zaštićeni, kao što je definirano standardom PCI DSS (engl. *Payment Card Industry Data Security Standard*).

Scenarij S5 primjer je uzorka na ulazu u neuronsku mrežu koji nije istreniran, a sadrži samo e-mail adresu korisnika. Ocjena razine rizika predložene neuronske mreže je srednje visoka (0.43), što se u potpunosti podudara s našim ranijim pretpostavkama. E-mail adresa je najrašireniji medij za kontakt između napadača i korisnika. Podatak o poznatoj e-mail adresi korisnika tretira se kao srednje rizičan jer ipak zahtijeva daljnje akcije od strane korisnika kako bi prijevara bila uspješno provedena u djelo. Primjeri scenarija zasnovanih na e-mailu vrlo su slični onima iz scenarija S2, iako valja napomenuti da postoji čitav niz prijevara koje se oslanjaju isključivo na korisnikovu e-mail adresu, barem u početku. Jedan zanimljiv primjer nedavno se pojavio u Hrvatskoj - napadači su objavili lažne oglase putem kojih su nudili vrlo povoljne ponude, uglavnom u vezi prodaje motornih vozila. Nakon što bi korisnik putem telefona ili e-maila kontaktirao napadače, oni su saznali njegove kontakt podatke i interese. Ako korisnik prihvati ponudu, naknadno je prisiljen platiti veliki iznos novca kako bi mu dogovorena roba bila isporučena, iako ona u stvarnosti uopće ne postoji.

Scenarij S6 još je jedan scenarij s brojem mobitela, vrlo sličan scenariju S3, ali s manje poznatih ostalih privatnih podataka. Rizik se u ovom slučaju procjenjuje na 0.62 što je tek nešto niža razina rizika od 0.66 u scenariju S3, i što se ubraja u srednju razinu rizika povrede privatnosti. Primjeri scenarija u stvarnom svijetu ponovno su vrlo slični primjerima scenarija S3, pogotovo primjer povratne SMS prijave koja zahtijeva poznavanje jedino broja mobitela.

U scenariju S7 izvršena je procjena rizika javno dostupnog profila društvene mreže. Prema trening skupu, ovaj je parametar ocijenjen kao srednja razina rizika za privatnost korisnika s aktivacijom vrijednosti od 0.64 na izlazu neuronske mreže. Međutim, činjenica je da privatne

podatke koje vlasnik profila društvene mreže javno dijeli na svom profilu mogu predstavljati čak i veći rizik od inicijalne procjene. Količina privatnih podataka koje su korisnici spremni podijeliti s javnosti itekako ovisi o njihovoj svijesti o mogućim rizicima koje takvo otkrivanje može prouzročiti.

Scenarij S8 odnosi se na slučaj kada su ime i broj kreditne kartice korisnika poznati napadaču. Zbog nazočnosti broja kreditne kartice scenarij je ocijenjen kao visoko rizičan po privatnost korisnika jer napadač može izazvati ozbiljne financijske gubitke bez intervencije korisnika. Primjeri scenarija u stvarnom svijetu vrlo su slični primjerima scenarija S4 i obično su rezultat ciljane povrede podataka u okviru sustava davatelja usluga.

### **3.5. Zaključak**

Komunikacijske usluge putem Interneta otvaraju korisnicima nove mogućnosti, ali također i nove opasnosti za njihovu sigurnost i privatnost. Privatnost korisnika na Internetu ugrožena je zbog niza sigurnosnih prijetnji. Glavni problem, osim ograničenja tehničkih metoda za zaštitu privatnih podataka, je niska razina svijesti korisnika o mogućim prijevarama na Internetu. Ovaj izvještaj predstavlja nastavak rada na kalkulatoru za procjenu rizika povrede privatnosti, a čiji cilj je korisnike upoznati s mogućim opasnostima te potaknuti angažman stručne javnosti za stvaranje novih regulatornih okvira povrede privatnosti na Internetu.

U radu se predlaže model kalkulatora koji na temelju ulaznih parametara koje zahtijevaju različite web-usluge pokušava procijeniti mogući rizik povrede privatnosti korisnika, ako su ti podaci procurili ili ih napadač nastoji zloupotrijebiti na bilo koji način. Nadalje, s obzirom da se kalkulator zasniva na neuronskoj mreži koja je sposobna učiti, izvršen je trening kalkulatora na odabranom skupu ulaznih podataka, a zatim i evaluacija na testnom skupu kako bi se procijenilo koliko dobro kalkulator vrši procjenu rizika povrede privatnosti. Pokazano je da kalkulator uspješno procjenjuje rizike za kombinacije ulaznih korisničkih parametara prema njihovoj sličnosti s poznatim, odnosno naučenim, kombinacijama parametara.

Uz procjenu rizika, kalkulator daje i tekstualne opise najčešćih prijevara. Predstavljajući česte prijevare u čitljivom i na ljudima razumljiv način, kalkulator doprinosi razvoju veće svijesti korisnika o potencijalnim rizicima povrede privatnosti. Budući rad na ovom projektu biti će usmjeren na širenje baze prijevara i njena integracija u kalkulator rizika. Osim toga, usredotočiti ćemo se na razvoj dodatne programske logike koja će biti u mogućnosti bolje obraditi nove kombinacije ulaznih parametara koji mogu biti potrebni u budućnosti, pogotovo u kontekstu aplikacija i usluga za pokretne uređaje.

### 3.6. Literatura

- [1] Ponemon Institute, “2013 Cost of Cyber Crime Study: United States”, 2013.
- [2] “Internet Usage Statistics”, Internet: <http://www.internetworldstats.com/stats.htm> [Jun. 24, 2014].
- [3] Mcaffe's Center for Strategic and International Studies, “The Economic Impact of Cybercrime and Cyber Espionage”, 2013.
- [4] T. Moore and R. Clayton, “An empirical analysis of the current state of phishing attack and defence”, in Proc. 2007 Workshop on the Economics of Information Security, 2007.
- [5] E. Kirda and C. Kruegel, “Protecting Users Against Phishing Attacks with AntiPhish”, in Proc. 29th Annual International Computer Software and Applications Conference, 2005, pp. 517-524.
- [6] R. Shah et al, “A Proactive Approach to Preventing Phishing Attacks Using Pshark”, in Proc. Sixth International Conference on Information Technology: New Generations, 2009, pp. 915-921.
- [7] V. Garg and S. Nilizadeh, “Craigslist Scams and Community Composition: Investigating Online Fraud Victimization”, in Proc. 2013 IEEE Security and Privacy Workshops, 2013, pp. 123-126.
- [8] J. Wang et al, “Phishing Susceptibility: An Investigation Into the Processing of a Targeted Spear Phishing Email”, IEEE Transactions on Professional Communication, vol. 55, no. 4, pp. 345-362, Dec. 2012.
- [9] F. Ahmed and M. Abulaish, “An MCL-Based Approach for Spam Profile Detection in Online Social Networks”, in Proc. 11th International Conference on Trust, Security and Privacy in Computing and Communication, 2012, pp. 602-608.
- [10] M. Sharifi et al, “Detection of Internet scam using logistic regression”, in Proc. 2011 IEEE International Conference on Systems, Man, and Cybernetics, 2011, pp. 2168-2172.
- [11] “ISO/IEC 27005:2011”, Internet: [http://www.iso.org/iso/home/store/catalogue\\_ics/catalogue\\_detail\\_ics.htm?csnumber=56742](http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=56742) [Jun. 24, 2014].
- [12] “ISO/IEC 27001:2013”, Internet: [http://www.iso.org/iso/home/store/catalogue\\_ics/catalogue\\_detail\\_ics.htm?csnumber=54534](http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=54534) [Jun. 24, 2014].
- [13] M. Mateski et al, “Cyber Threat Metrics”, Sandia National Laboratories, 2012.
- [14] “Prolexic DDoS Downtime Calculator”, Internet: <http://www.prolexic.com/ddos-downtime-calculator/linkedin.html> [Jun. 24, 2014].

- [15] X. Chen et al, “Quantitative threat assessment of denial of service attacks on service availability”, in Proc. 2011 International Conference on Computer Science and Automation Engineering, 2011, pp. 220-224.
- [16] “Symantec Cyber Resilience Assessment”, Internet: <https://scm.symantec.com/cyberresilientassessment/en/?mt=1404cyberesiliencesymcomsite&loc=APAC> [Jun. 24, 2014].
- [17] “Symantec Severity Assessment: Threats, Events, Vulnerabilities, Risks”, Internet: <https://www.symantec.com/content/en/us/about/media/securityintelligence/SSR-Severity-Assesment.pdf>, Feb. 2006 [Jun. 24, 2014].
- [18] “OWASP Risk Assessment Calculator”, Internet: <http://paradoslabs.nl/owaspcalc/> [Jun. 24, 2014].
- [19] “OWASP Risk Rating Methodology”, Internet: [https://www.owasp.org/index.php/How\\_to\\_value\\_the\\_real\\_risk\\_AoC](https://www.owasp.org/index.php/How_to_value_the_real_risk_AoC) [Jun. 24, 2014].
- [20] “University Unveils Cyber Threat Calculator”, Internet: <http://www.informationweek.com/university-unveils-cyber-threat-calculator/d/did/1051207> [Jun. 24, 2014].
- [21] A.Y. Keren and K. Elazari, “Internet as a CII - A framework to measure awareness in the cyber sphere”, in Proc. 4th International Conference on Cyber Conflict, 2012, pp. 1-13.
- [22] I. Bose and A.C.M. Leung, “A comparative study of anti-phishing preparedness of Hong Kong and Singapore banks”, in Proc. 2007 International Conference on Industrial Engineering and Engineering Management, 2007, pp. 1893-1897.
- [23] European Union Agency for Network and Information Security, “ENISA Threat Landscape 2013”, 2013.
- [24] “EU Directive 2002/58/EC”, Internet: <http://eur-lex.europa.eu/lexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML>, Jul. 12, 2002 [Jun. 24, 2014].
- [25] J. Isacenkova et al, “Inside the SCAM Jungle: A Closer Look at 419 Scam Email Operations”, in Proc. 2013 IEEE Security and Privacy Workshops, 2013, pp. 143-150.

## 4. Simulacija načina rada i usporedba značajki sustava DVB-T i DVB-T2

### 4.1. Sažetak

U ovom izvješću analizirane su pozitivne strane povećanja brzine prijenosa u zemaljskom radiodifuzijskom sustavu prilikom prelaska sa sustava DVB-T na sustav DVB-T2. Uspoređene su zahtijevane minimalne vrijednosti omjera nositelj/šum (engl. *Carrier to Noise Ratio*) za prijam bez pogrešaka u sustavu DVB-T i sustavu DVB-T2 uz parametre odašiljanja slične onima koji se trenutno koriste u Hrvatskoj. C/N je izračunat korištenjem simulacija razvijenih u programskom paketu Matlab, za tri najčešće korištena modela kanal: Gaussov, Riceov i Rayleighov kanal. Rezultati pokazuju povećanje korisne brzine prijenosa za približno 63% bez značajnog povećanja minimalno potrebnog C/N. Uporabom novih tehnika videokompresije i statističkog multipleksiranja u velikim multipleksima, zaključeno je da je moguće odašiljanje i do 10 puta većeg broja televizijskih programa uz održavanje zahtijevane kvalitete prijema i uz istu korištenu širinu frekvencijskog pojasa.

## 4.2. Uvod

Prelaskom s analognog na digitalno odašiljanje zemaljskih televizijskih programa koji je u Hrvatskoj završen 5. listopada 2010. godine, ugašena je analogna radiodifuzija televizijskih programa i trenutno se svi televizijski programi odašilju putem digitalnih televizijskih sustava. Proces prijelaza s analogne na digitalnu televiziju proveden je u skladu sa „Strategijom prelaska s analognog na digitalno emitiranje televizijskih programa u Republici Hrvatskoj“ 0 koju je Vlada RH donijela 31.07.2008. godine pri čemu je temeljni cilj definiran na sljedeći način: „Vlada Republike Hrvatske utvrđuje, kao glavni strateški cilj u razdoblju do 31. prosinca 2010. godine, potpuni prelazak s analognog na digitalno emitiranje televizijskih programa u Republici Hrvatskoj.“ Prestankom rada analognih odašiljača u zemaljskom radiodifuzijskom sustavu u frekvencijskim pojasevima VHF III i UHF IV/V, oslobađa se dio radiofrekvencijskog (RF) spektra koji se može rabiti za dodatne televizijske programe, mobilne komunikacijske usluge, širokopojasni pristup Internetu, radiomikrofone te druge elektroničke komunikacijske usluge. Oslobodeni dio spektra naziva se „digitalna dividenda“. U „Strategiji prelaska s analognog na digitalno emitiranje televizijskih programa u Republici Hrvatskoj“ pojas 790-862 MHz nije zauzet radiodifuzijskim uslugama (slika 2.1.). Završetkom procesa prelaska s analogne na digitalnu radiodifuziju televizijskih programa u zemaljskoj mreži, ovaj pojas postaje raspoloživ za nove elektroničke komunikacijske usluge. Digitalna dividenda definirana je kao dio radiofrekvencijskog spektra oslobođen nakon prelaska s analognog na digitalno emitiranje televizijskih programa. Digitalna dividenda nije samo pojas 790-862 MHz već se digitalnom dividendom može smatrati razlika između količine spektra potrebne za prijenos televizijskih programa u analognoj tehnologiji i količine spektra potrebne za prijenos istog broja programa u digitalnoj tehnologiji uz održavanje približno jednake kvalitete slike. Stoga se oslobođeni dio spektra od 790-862 MHz zove „prva digitalna dividenda“ i danas njome koriste dva nacionalna mobilna operatora koji taj dio spektra rabe za širokopojasne mobilne usluge putem sustava LTE (engl. *Long Term Evolution*, LTE).

„Strategijom prelaska s analognog na digitalno emitiranje televizijskih programa u Republici Hrvatskoj“ za sustav zemaljske radiodifuzije televizijskih programa odabran je sustav DVB-T (engl. *Digital Video Broadcasting - Terrestrial*), 0, a kao norma za kompresiju videosignala odabrana je norma MPEG-2 (engl. *Motion Pictures Experts Group*), 0.

Sustav DVB-T razvijen je okviru rada na Rad na Projektu za radiodifuziju digitalnog videosignala (engl. *Digital Video Broadcasting Project*, DVB Project) započeo je u Europi 1993. godine i imao je za cilj odrediti okvir za primjenu MPEG-2 televizijskih usluga. U okviru DVB projekta su se udružili vodeći proizvođači televizijske opreme, operatori mreža, radiodifuzijske organizacije, regulatorna tijela, proizvođači softvera i ostali zainteresirani, kako bi razvili specifikacije za prijenos MPEG-2 prijenosnog podataka do krajnjih korisnika. Rad u okviru DVB projekta u prvoj fazi rezultirao je ETSI (engl. *European Telecommunications Standards Institute*) normama za radiodifuziju digitalnog videosignala putem satelitskih komunikacija (engl. *DVB-Satellite*, DVB-S) 0, sustava kabela televizije (engl. *DVB-Cable*, DVB-C) 0, i sustava zemaljske radiodifuzije (engl. *DVB-Terrestrial*, DVB-T), 0.



Kanal	21	55	56	60	61	69	70
Radijska frekvencija	470MHz		750MHz		790MHz		860MHz
Vrsta usluge	DVB-T/H		DVB-T		IMT		
MUX A – državni	5×SDTV*						
MUX B – državni	5×SDTV**						
MUX C – državni	raspoloživo: 5×SDTV						
MUX D – regionalni/ državni	1 – 3×SDTV*** + raspoloživo: 2 – 4 SDTV (regionalni/državni)						
MUX E – državni	DVB-H: raspoloživo oko 30 TV programa ili oko 60 radijskih programa						
MUX F – državni/ regionalni	raspoloživo: DVB-T ili DVB-H						
MUX G – regionalni/ državni	raspoloživo: DVB-T ili DVB-H						
MUX H – regionalni	raspoloživo: DVB-T ili DVB-H						

- \* Namijenjeno za opće i/ili specijalizirane TV programe javne televizije (Hrvatska radiotelevizija)
- \*\* Namijenjeno za opće i/ili specijalizirane TV programe komercijalnih nakladnika televizije na državnoj razini
- \*\*\* Namijenjeno za opće TV programe postojećih komercijalnih nakladnika televizije na razinama nižima od državne razine

### Slika 2.1. Raspoloživi multipleksi i radiodifuzijske usluge u pojasevima UHF IV

MPEG je skraćeni naziv za Skupinu stručnjaka za pokretne slike. Skupina MPEG osnovana je 1988. godine u okviru ISO/IEC (engl. *International Standards Organisation/International Electrotechnical Commission*) s ciljem razvoja i definiranja norme za kompresiju videosignala i pratećih tonskih signala. Prva norma proizašla iz rada MPEG skupine poznata kao norma MPEG-1, bila je namijenjena pohranjivanju videosignala na CD-ROM i nije bila prikladna za radiodifuzijske i televizijske primjene. Druga norma razvijena u okviru MPEG skupine ima naziv ISO/IEC IS 13818-Informacijska tehnologija - Generičko kodiranje pokretnih slika i pratećih audiosignala (engl. *Generic Coding of Moving Pictures and Associated Audio*), i poznata je kao norma MPEG-2 0. Norma specificira skup postupaka kodiranja s jezgrom sustava koja sadrži algoritam kodiranja standardnih televizijskih formata (engl. *Standard Definition Television, SDTV*) za brzine prijenosa od 4-10 Mbit/s kojima se može postići kvaliteta prijamnih signala slična kao u analognim sustavima. Predloženi postupci kodiranja imaju takva svojstva da ih je moguće primijeniti i na televiziju visoke kvalitete (engl. *High Definition Television, HDTV*) uz brzine prijenosa oko 20 Mbit/s.

U prvom dijelu navedene norme ISO/IEC IS 13818-1: *Generic coding of moving pictures and associated audio information - Part 1: Systems*, određen je način oblikovanja MPEG-2 prijenosnog toka podataka (engl. *Transport Stream, TS*) čime je otvorena mogućnost kombiniranja više osnovnih tokova podataka (video, audio, tekst, grafika, mirne slike i dr.), u jedan ili više tokova pogodnih za prijenos i pohranjivanje, 0. Oblikovanjem prijenosnog toka podataka više televizijskih programa može se multipleksirati u jedan tok podataka i prenositi jednim televizijskim kanalom.

Od normi razvijenih nakon MPEG-2 norme, za digitalnu televiziju posebno značenje ima norma ISO/IEC IS 14496-10 Kodiranje audio-vizualnih objekata - dio 10: Poboľjšano kodiranje videosignala (*Coding of Audio-Visual Objects - Part 10: Advanced Video Coding*), 0, usvojena 2002. godine. Norma je uključena u ITU-T preporuke kao preporuka ITU-T H.264 pod nazivom *Advanced Video Coding for Generic Audiovisual Services*. Norma je poznata i pod nazivom H.264/AVC (engl. *Advanced Video Coding, AVC*). Algoritam kompresije je složeniji u odnosu na MPEG-2, ali pruža mogućnost postizanja dvostruko većih stupnjeva kompresije za istu kvalitetu slike što je posebno važno za HDTV.

Početakom 2013. dovršena je nova norma za kompresiju videosignala ITU-T H.265 / ISO/IEC 23008-2 Visokoučinkovito kodiranje i dostava medijskih sadržaja u heterogenim okruženjima - dio 2: Visokoučinkovito kodiranje videosignala (engl. *High efficiency coding and media delivery in heterogeneous environments - Part 2: High efficiency video coding*), 0. Norma je poznata pod skraćenicom HEVC (engl. *High Efficiency Video Coding*). HEVC omogućava udvostručenje stupnja kompresije u odnosu na H.264/AVC uz održavanje iste kvalitete slike. Podržava rezolucije slike sve do 8k UHD (engl. *Ultra High Definition*) tj. prostorni format do 8192x4320 elemenata slike u slici.

DVB projekt nakon početnog uspjeha nastavio je sa svojim radom tako da je razvijena druga generacija ETSI normi za radiodifuziju u koju pripadaju druga generaciju satelitskih sustava (DVB-S2) 0, druga generacija sustava za zemaljsku radiodifuziju (DVB-T2) 0 i druga generacija sustava digitalnu kabelsku televiziju (DVB-C2) 0.

Poboľjšanja druge generacije ETSI normi u odnosu na prvu generaciju sastoje se u sljedećem:

- povećana je spektralna djelotvornost uporabom složenijih modulacijskih postupaka što ima za posljedicu povećanje korisne brzine prijenosa i bolje iskorištenje raspoložive širine frekvencijskog pojasa (u pojedinom kanalu može se prenositi veći broj TV programa);
- poboľjšane su tehnike zaštite od pogrešaka tako da je moguće postići izvrsnu kvalitetu prijamnog signala i u uvjetima djelovanja visokih razina šuma i interferencije u kanalu;
- povećan je broj parametara sustava koji mogu biti odabrani u postupku zaštite od pogrešaka i modulacije čime se postiže veća fleksibilnost sustava i mogućnost prilagodbe različitim namjenama, uvjetima u kanalu i vrstama usluga.

U Hrvatskoj je digitalna zemaljska televizija podijeljena u devet jednofrekvencijskih mreža (engl. *Single Frequency Network, SFN*). U svakoj jednofrekvencijskoj mreži trenutno se rabi pet multipleksa: multipleks A i multipleks B za besplatne nacionalne programe (engl. *Free-to-air, FTA*), multipleks D za besplatne nacionalne i regionalne programe te multipleksi C i E za uslugu naplatne televizije (engl. *pay-TV*). Multipleksi A, B i D odašilju signale u normi DVB-T, a multipleksi C i E koriste normu DVB-T2. U multipleksima C i E, četiri regije su spojene u dva dijela, koje praktično rezultiraju u sedam jednofrekvencijskih mreža.

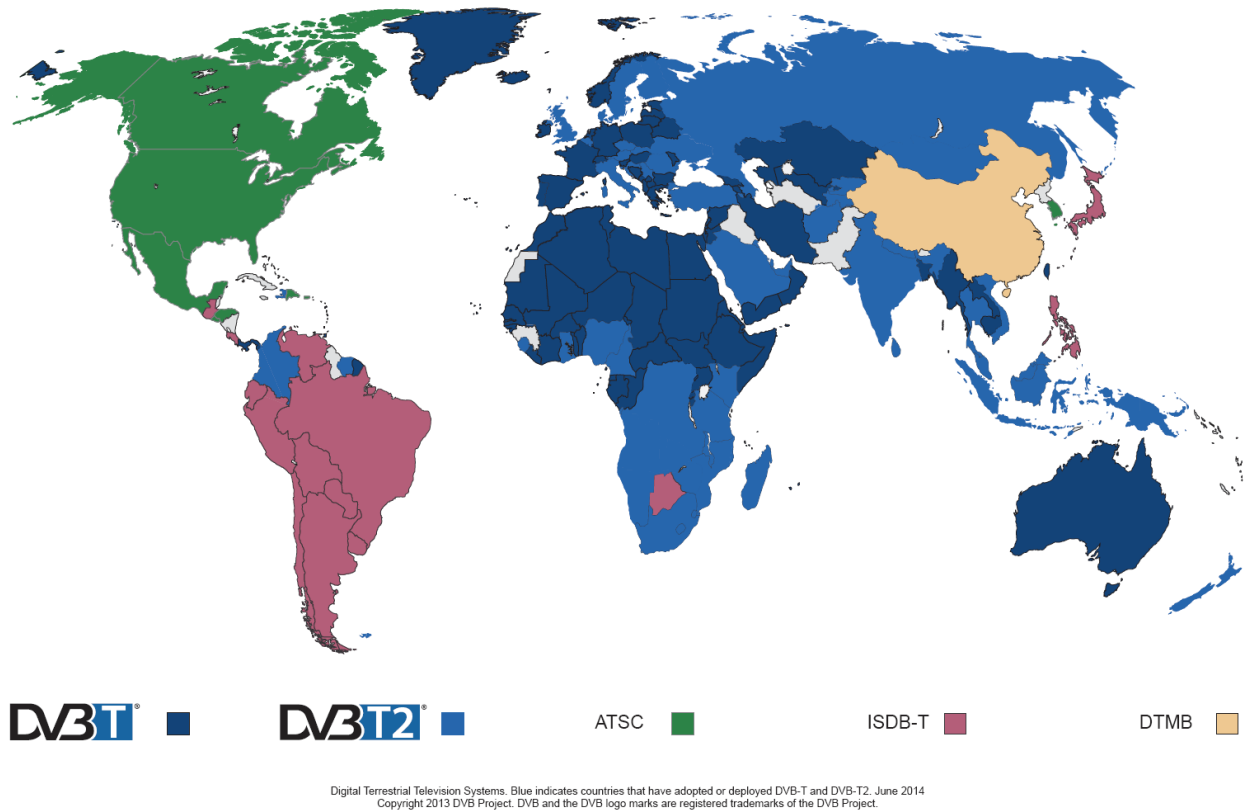
Preporukom Europske komisije 0, početak 2012. godine bio određen kao krajnji rok za prestanak analognog emitiranja televizijskih programa u svim zemljama članicama EU-a. Većina članica EU taj rok je ispoštovala. Prestanak rada analognih TV odašiljača u ostalim europskim zemljama planiran je do 2015. godine. Tablica 2.1. prikazuje podatke o početku i završetku implementacije sustava digitalne zemaljske televizije u europskim zemljama.

**Tablica 2.1.** Stanje implementacije DVB-T sustava u europskim zemljama (izvor: DigiTAG, <http://www.digitag.org/>, pristup: rujan, 2014.)

Država	Početak digitalnog emitiranja	Postupak kompresije	Gašenje analognih odašiljača
Ujedinjeno Kraljevstvo	1998.	MPEG-2	24. listopada 2012.
Švedska	1999.	MPEG-2	29. listopada 2007.
Španjolska	2000.	MPEG-2	3. travnja 2010.
Finska	2001.	MPEG-2	1. rujna 2007.
Švicarska	2001.	MPEG-2	26. studenog 2007.
Njemačka	2002.	MPEG-2	25. studenog 2008.
Belgija	2002.	MPEG-2	1. ožujka 2010.
Nizozemska	2003.	MPEG-2	11. prosinca 2006.
Italija	2004.	MPEG-2	30. lipnja 2012.
Francuska	2005.	MPEG-2/MPEG-4 AVC	28. studenoga 2011.
Češka Republika	2005.	MPEG-2	4. studenoga 2011.
Danska	2006.	MPEG-2/MPEG-4 AVC	1. studenoga 2009.
Estonija	2006.	MPEG-4 AVC	1. srpnja 2010.
Austrija	2006.	MPEG-2	7. srpnja 2011.
Slovenija	2006.	MPEG-4 AVC	1. prosinca 2010.
Norveška	2007.	MPEG-4 AVC	1. prosinca 2009.
Litva	2008.	MPEG-4 AVC	29. listopada 2012.
Mađarska	2008.	MPEG-4 AVC	31. listopada 2013.
Ukrajina	2008.	MPEG-4 AVC	2014.
Latvija	2009.	MPEG-4 AVC	1. lipnja 2010.
Portugal	2009.	MPEG-4 AVC	26. travnja 2012.
Hrvatska	2009.	MPEG-2	5. listopada 2010.
Poljska	2009.	MPEG-4 AVC	22. srpnja 2013.
Slovačka	2009.	MPEG-2	31. prosinca 2012.
Irska	2010.	MPEG-4 AVC	24. listopada 2012.
Rusija	2012.	MPEG-4 AVC	Nije definiran datum.

Hrvatska je 15. zemlja u Europi koja se prebacila s analogne na digitalnu televiziju, a zbog takvo rane digitalizacije uveden je sustav DVB-T koji koristi MPEG-2 kompresiju, iako su tada već postojale norme za napredniji DVB-T2 sustav, kao i napredniji H.264/AVC (MPEG-4 Part 10) postupak kompresije videosignala, koji se može koristiti i u sustavu DVB-T. Takav pristup su koristile i druge zemlje koje su imale ranu digitalizaciju, prvenstveno zbog nekoliko puta veće cijene prijamnika (engl. *Set Top Box*, STB) i televizora s novijim H.264/AVC tipom dekodera. DVB-T2 TV uređaji ili prijammnici nisu bili dostupni na tržištu u

to vrijeme. Trenutačno 24 zemlje svijeta (uključujući i Hrvatsku) komercijalno koriste sustav DVB-T2, dok ga još 10 zemalja koristi eksperimentalno ili ga tek planira koristiti, slika 2.2., 0.



**Slika 2.2.** Implementacija normi za zemaljsku radiodifuziju

(izvor: [https://www.dvb.org/resources/public/images/site/dvb-t\\_map.pdf](https://www.dvb.org/resources/public/images/site/dvb-t_map.pdf), pristup: rujan 2014.)

Zbog visoke spektralne učinkovitosti sustava izvedenih u skladu s normom DVB-T2, viših stupnjeva kompresije novijih videokodera (H.264/AVC i posebno HEVC u odnosu na MPEG-2) te bolje učinkovitosti statističkog multipleksiranja u velikim multipleksima, vjerojatno će multipleksi za besplatne nacionalne i regionalne programe migrirati na noviju normu DVB-T2 koja se već koristi za uslugu naplatne televizije u Hrvatskoj. Također, uvođenjem sustava DVB-T2, još jedan dio frekvencijskog spektra će vjerojatno postati slobodan, te će se moći koristiti za širokopojsne mobilne usluge ili za neke druge svrhe.

Izvešće je organizirano na sljedeći način. Nakon sažetka i uvoda, treće potpoglavlje daje pregled radova vezanih uz tematiku prelaska sa sustava DVB-T na sustav DVB-T2. Četvrti dio opisuje glavne tehničke karakteristike sustava DVB-T i DVB-T2. Peti dio objašnjava tri najčešće korištena modela kanala koji će se koristiti u kasnijim simulacijama. Šesti dio objašnjava dobivene rezultate simulacija, sa sličnim parametrima poput postojećih DVB-T i DVB-T2 hrvatskih multipleksa. U sedmom dijelu, raspravljat će se o dobitku u broju TV kanala i na kraju se iznose zaključci rada.

### 4.3. Pregled ostalih radova

U 0 autori su razmotrili značajke sustava DVB-T i DVB-T2 te su analizirali mogućnost prijelaza sa sustava DVB-T na sustav DVB-T2 u Hrvatskoj. Dijelovi toga rada prezentirani su i u ovom izvješću. U 0 autori su analizirali digitalnu dividendu nakon prelaska na DVB-T2, kao i značajke sustava DVB-T2 te mogućnost uporabe H.264/AVC videokompresije. U radu 0 dan je detaljan pregled sustava DVB-T2, zajedno sa prednostima i nedostacima. Ovaj članak također predstavlja sveobuhvatan pregled laboratorijskih i terenskih mjerenja te njihovih rezultata u Španjolskoj i na sjeveru Njemačke. U 0 autori raspravljaju o mogućem napretku OFDM (engl. *Orthogonal Frequency Division Multiplexing*) sustava pomoću odašiljanja signala brže od Nyquistovog ograničenja (engl. *Faster-Than-Nyquist*, FTN), što može poboljšati mnoge postojeće i nadolazeće širokopojasne tehnologije pristupa kao što su WLAN, LTE i DVB. Sličan je rad predstavljen u 0, gdje su autori su zaključili da FTN može prenijeti i do dva puta veću količinu podataka u odnosu na običnu modulaciju uz istu energiju bita, jednaku širinu korištenog frekvencijskog spektra i istu vjerojatnost pogreške. Metoda se može izravno koristiti za OFDM i kvadraturnu amplitudnu modulaciju (engl. *Quadrature Amplitude Modulation*, QAM).

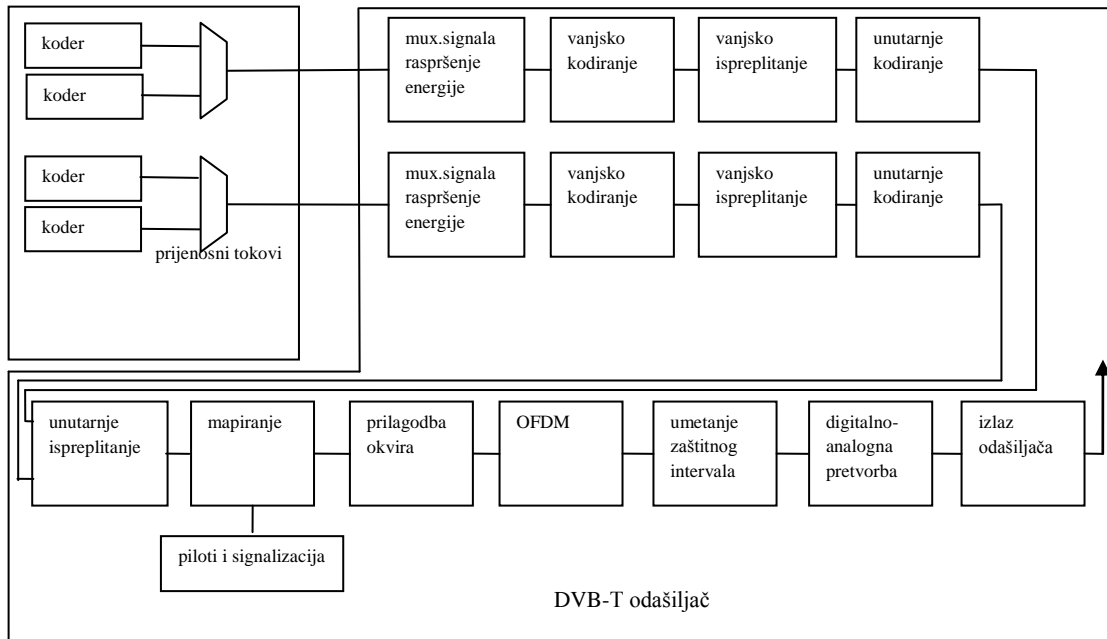
U 0, autori su analizirali DVB-T i DVB-T2 sustav za fiksni prijam zemaljskih televizijskih kanala, pomoću klasičnog Riceovog i Rayleighovog modela kanala s 20 nezavisnih zraka. U 0, autori su procijenili izvedbu DVB-T2 SFN mreže i usporedili s DVB-T mrežom, sa sličnim parametrima kao što su u njihovoj zemlji (Francuska).

### 4.4. Tehnički opis sustava DVB-T i DVB-T2

DVB-T odašiljač prikazan na slici 2.3. sastoji se od nekoliko blokova obrade signala 0, 0: izvorno kodiranje i MPEG-2 multipleksiranje, razdjelnik, multipleksiranje signala i raspršenje energije, vanjsko kodiranje (Reed-Solomonovo kodiranje), vanjsko ispreplitanje (konvolucijsko ispreplitanje), unutarnje kodiranje (konvolucijsko kodiranje), unutarnje ispreplitanje, dodjela bita simbolima, dodavanje pilotskih nositelja i nositelja za signalizaciju parametara sustava (engl. *Transmission Parameter Signaling*, TPS), OFDM multipleksiranje i umetanje zaštitnog intervala, DAC (digitalno-analogni pretvarač) i izlaz odašiljača (engl. *RF front end*).

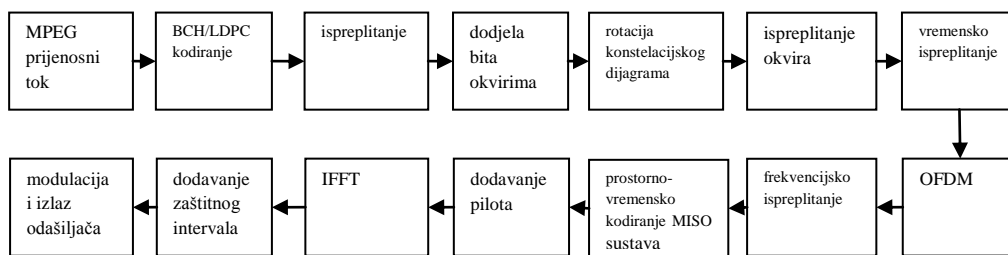
Prijamnik koristi tehnike koje su dvojne onima koji se koriste u prijenosu. Njegov praktični rad ovisi o hardverskoj izgradnji (nije standardiziran kao odašiljač).

U Hrvatskoj, DVB-T sustav se trenutno koristi za nekoliko nacionalnih i regionalnih televizijskih kanala. Prijenosni parametri koji se koriste u multipleksima A i B su sljedeći: 64-QAM, omjer koda 3/4, zaštitni interval 1/4, MPEG-2 videokompresija, 8k FFT uz korisnu brzinu prijenosa od 22,4 Mbit/s. U multipleksu D, ovisno o regiji, mogu biti korišteni neki drugi parametri prijenosa, ovisno o području i broj regionalnih TV kanala. Kasnije u radu, parametri koji se koriste u multipleksima A i B bit će korišteni za usporedbu sa sustavom DVB-T2.



Slika 2.3. Blok dijagram DVB-T odašiljača

Glavna prednost sustava DVB-T2 u usporedbi s DVB-T je povećanje kapaciteta digitalne zemaljske televizije, 0. DVB-T2 pruža minimalni porast brzine prijenosa od približno 30% u odnosu na DVB-T u istim uvjetima prijama. Iako je u osnovi prilagođen fiksnom prijama, sustav DVB-T2 je također moguće izvesti i za prijenosne ili mobilne uređaje, ako se koristi odgovarajući skup parametara odašiljanja.



Slika 2.4. Blok dijagram DVB-T2 odašiljača

Odašiljač DVB-T2 sustava prikazan na slici 2.4. sastoji se od nekoliko blokova obrade signala. Prva novost u sustavu DVB-T2 je poboljšana tehnika zaštite od pogrešaka, utemeljena na LDPC/BCH (engl. *Low Density Parity Check/ Bose-Chaudhuri-Hocquengham*) kodiranju 0, koja se koristi kao zaštita od smetnji i šuma. Ovo zaštitno kodiranje nudi izvrsne performanse što rezultira vrlo robusnim prijamom signala u raznim uvjetima prijenosa signala, kao i povećanje brzine prijenosa.

Osim toga, nova tehnika rotacije konstelacijskog dijagrama rezultirala je poboljšanom robusnosti protiv gubitaka podataka. Ova tehnika je vrlo važno za postizanje bolje performanse u težim uvjetima rasprostiranja signala, jer osigurava da se gubitak informacije iz

jedne komponente signala može nadoknaditi drugom komponentom signala. Ovom tehnikom se stanja QAM modulacije rotiraju u I-Q ravnini, gdje se Q komponenta šalje u različitim vremenskim trenucima koristeći različite okvire. Kutovi rotacije su eksperimentalno utvrđeni da su  $29^\circ$ ,  $16,8^\circ$ ,  $8,6^\circ$  i  $3,6^\circ$  za QPSK, 16-QAM, 64-QAM i 256-QAM 0.

Isto kao i kod DVB-T, DVB-T2 sustav koristi kodirani ortogonalni frekvencijski multipleks (COFDM), s novo uvedenom modulacijom po podnosiocu - 256-QAM. To dopušta veći broj bitova koji se mora provesti na podataka stanica, čime se povećava učinkovitost prenošenja i brzinu prijenosa. Uvedena je i podrška za 16K i 32K FFT čime se povećala duljina trajanja zaštitnog intervala bez smanjenja spektralna učinkovitosti sustava, jer je veće trajanje korisnog OFDM simbola, u odnosu na 8K mod. To omogućava veću SFN mrežu (engl. *Single Frequency Network*) u DVB-T2 sustavu. Alternativno, zaštitni interval u 32K modu jednakog apsolutnog trajanja kao u 8K modu omogućava veće korisno trajanje OFDM simbola u 32K modu.

Također je moguće birati između normalnog ili proširenog načina odašiljanja. Prošireni mod odašiljanja daje mogućnost korištenja više podnosioca po simbolu koja rezultira povećanom brzinom prijenosa podataka, bez povećavanja širine kanala.

Kako bi se kompenzirale vremenske i frekvencijske promjene u kanalima, DVB-T2 koristi raspršene pilote. Dodatna fleksibilnost u odnosu na DVB-T pruža mogućnost izabrati jednu od osam uzoraka odašiljanja raspršenih pilota, ovisno o odabranoj FFT veličini i zaštitnom intervalu, kako bi se povećala korisna brzina prijenosa. Međutim, moguće su samo neke kombinacije zaštitnih intervala, FFT veličina i uzoraka odašiljanja pilota.

Svaka usluga može imati različite robusnost i razinu zaštite s pripadajućom modulacijom korištenjem odvojenih logičkih kanala na fizičkom sloju, (engl. *Physical Layer Pipes*, PLP). Svaki PLP nosi jedan ili više logičkih tokova podataka, a može imati različite fizičke parametre, kao što su parametri kodiranja radi zaštite od pogrešaka, modulacijski postupak za podnosioc, brzina prijenosa prijenosnog toka podataka i stupanj ispreplitanja. DVB-T2 omogućuje prijenos više PLP-ova istovremeno.

Jednostavna usporedba raspoloživih modova odašiljanja u DVB-T i DVB-T2 sustavu prikazana je u Tablici 2.2. Podebljani brojevi u DVB-T2 stupcu znači da su novouvedeni u ovom sustavu.

U Hrvatskoj, parametri koji se koriste u multipleksima C i E su: 256-QAM (rotirani), zaštitno kodiranje 2/3, zaštitni interval 19/256, četvrti uzorak odašiljanja pilota, 32k FFT (proširena) uz korisnu brzinu prijenosa 36,6 Mbit/s. Također, H.264/AVC se koristi kao videokompresija, zajedno sa statističkim multipleksiranjem. U usporedbi s MPEG-2, H.264/AVC je otprilike dvostruko učinkovitiji, uz zadržavanje iste vizualne kvalitete. Korištenjem multipleksiranja, ovisno o broju kanala u multipleksu, dobit može biti i do 50% (u usporedbi s konstantnom brzinom prijenosa) 0.

**Tablica 2.2.** Usporedba DVB-T i DVB-T2 sustava

	<b>DVB-T</b>	<b>DVB-T2</b>
<b>Kodiranje</b>	Konvolucijsko kodiranje +RS	LPDC+BCH 1/2, <b>3/5</b> , 2/3, 3/4, <b>4/5</b> , 5/6
<b>Modulacija</b>	QPSK, 16-QAM, 64-QAM	QPSK, 16-QAM, 64-QAM, <b>256-QAM</b>
<b>Zaštitni interval</b>	1/4, 1/8, 1/16, 1/32	1/4, <b>19/256</b> , 1/8, <b>19/128</b> , 1/16, 1/32,
<b>FFT veličina</b>	2K, 8K	<b>1K, 2K, 4K, 8K, 16K, 32K</b>
<b>Raspršeni piloti</b>	8% ukupno	<b>1%, 2%, 4%, 8%</b> ukupno
<b>Kontinuirani piloti</b>	2,6 % ukupno	<b>0,35%</b> ukupno

#### 4.5. Modeli kanala

DVB-T i DVB-T2 sustav smo usporedili korištenjem tri modela kanala: Gaussov, Riceov i Rayleighev model kanala. Gaussov model kanala opisuje samo jednu zraku optičke vidljivosti. Riceov kanal ima jednu izravnu zraku i nekoliko zakašnjelih zraka, dok Rayleighev kanal nema izravne zrake. Karakteristike Riceovog i Rayleighovog modela kanala mogu se naći u 0 i njihovi parametri dani su u Tablici 2.3.

**Tablica 2.3.** Normirana amplituda (ukupna snaga 0 dB), fazno i vremensko kašnjenje koji su korišteni za simulaciju Riceovog i Rayleighovog modela kanala

$I$	$\rho_i$ (Riceov)	$\rho_i$ (Rayleighev)	$\tau_i$ ( $\mu$ s)	$\theta_i$ (rad)
0	0.953462	-	0	0
1	0.016187	0.053687	1.003019	4.855121
2	0.049635	0.164620	5.422091	3.419109
3	0.114301	0.379093	0.518650	5.864470
4	0.085224	0.282656	2.751772	2.215894
5	0.072647	0.240941	0.602895	3.758058
6	0.017358	0.057568	1.016585	5.430202
7	0.042204	0.139975	0.143556	3.952093
8	0.014467	0.047981	0.153832	1.093586
9	0.051955	0.172315	3.324866	5.775198
10	0.112561	0.373324	1.935570	0.154459
11	0.083017	0.275336	0.429948	5.928383
12	0.098485	0.326639	3.228872	3.053023
13	0.073805	0.244784	0.848831	0.628578
14	0.063414	0.210321	0.073883	2.128544
15	0.048003	0.159207	0.203952	1.099463
16	0.042031	0.139401	0.194207	3.462951
17	0.067413	0.223585	0.924450	3.664773
18	0.032729	0.108549	1.381320	2.833799
19	0.062084	0.205908	0.640512	3.334290
20	0.072913	0.241824	1.368671	0.393889



Prilikom usporedbe DVB-T i DVB-T2 sustava, koristili smo 'idealnu procjenu kanala', što znači da se pilotski podnosioci zapravo nisu koristili za procjenu frekvencijskog odziva kanala. Umjesto toga, invertirana karakteristika 'poznatog' kanala pomnožena je s primljenim simbolima. Za manje degradacije u frekvencijskom odzivu kanala, C/N će biti sličan kao kod Gaussovog modela kanala, dok je za veće degradacije potreban viši omjer C/N. U mjerenjima u realnom kanala, minimalni omjer C/N trebao bi biti još veći od 0, jer u tom slučaju frekvencijski odziv kanala nije poznat, nego se računa pomoću pilotskih podnosioca. U nekim slučajevima, degradacije u kanalu mogu biti prevelike da bi mogli dekodirati signal, uz bilo koji C/N.

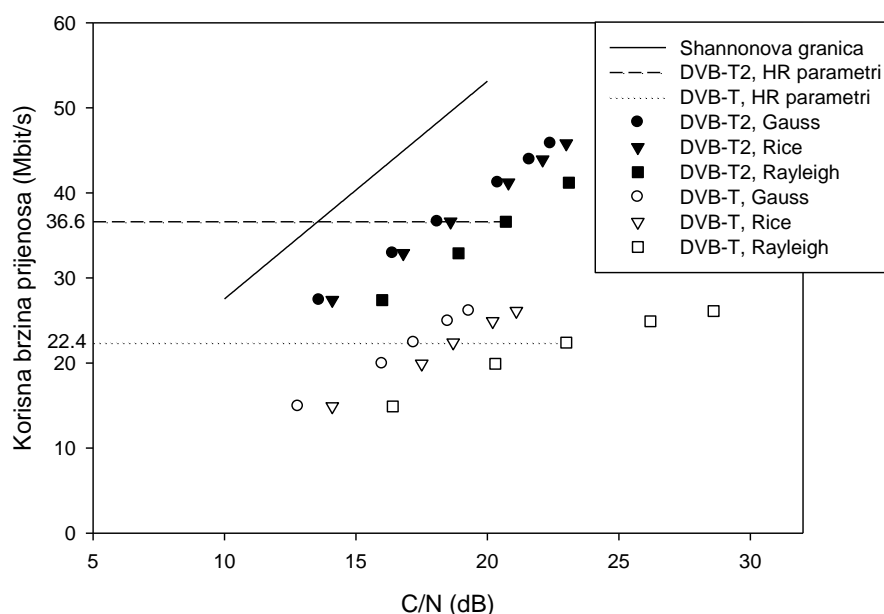
#### 4.6. Rezultati simulacije

Primjer povećanja korisne brzine prijenosa sa DVB-T na DVB-T2 sustav prikazan je na slici 2.5. Parametri koji se koriste u simulacijama:

- DVB-T: 64-QAM, zaštitni interval 1/4, FFT 8k; omjer zaštitnog koda: 1/2, 2/3, 3/4, 5/6 i 7/8;
- DVB-T2: 256-QAM (rotiran), zaštitni interval 19/256, FFT mod 32K (proširen), četvrti uzorak odašiljanja pilota; omjer zaštitnog koda: 1/2, 3/5, 2/3, 3/4, 4/5, 5/6; ostali parametri su isti kao u referentnom modelu DVB-T2 sustava V&V VV004-8KFFT 0.

Ispitane vrste kanala bile su, kako je opisano ranije, Gaussov, Riceov i Rayleighev model kanala. Za DVB-T, C/N omjer je dobiven iz 0 (simulacija je provedena u Matlabu, Simulink) za Gaussov i Riceov model, dok je za Rayleighev model kanala minimalni C/N preuzet iz 0. Za DVB-T2, C/N je izračunat pomoću DVB-T2 simulacije (engl. *Common Simulation Platform*, CSP), verzije 030202 0, također provedene u Matlabu. C/N vrijednosti predstavljaju minimalne vrijednosti za prijam bez pogrešaka (engl. *Quasi Error Free*, QEF), što znači omjer pogrešnih i ukupno prenesenih bitova (engl. *Bit Error Rate*, BER)  $< 2 \cdot 10^{-4}$  nakon unutarnjeg dekodera u DVB-T i BER  $< 10^{-7}$  nakon unutarnjeg dekodera u DVB-T2 sustavu.

Treba napomenuti da je zaštitni interval je postavljen na 1/4 u DVB-T sustavu, 8K modu, u Hrvatskoj, koji bi odgovarao zaštitnom intervalu 1/16 u DVB-T2, 32K mod, jer je korisno trajanje OFDM simbola 4 puta veće u 32K modu. Međutim, u Hrvatskoj se u DVB-T2 sustavu koristi zaštitni interval 19/256 tako da smo koristili tu vrijednost za DVB-T2 simulaciju (zaštitni interval 19/256 daje samo malo nižu korisnu brzinu prijenosa, u odnosu na 1/16). C/N omjer može biti nešto drugačiji, ako bi se koristili drugi simulatori ili stvarna mjerenja kanala. Međutim, može se naći da je sličan omjer C/N (uz korištenje parametara kao u Hrvatskoj) izračunat u 0 za DVB-T sustav i u 0 za DVB-T2 sustav. Na slici 2.5 uz ukupne rezultate, parametri koji se koriste u Hrvatskoj za DVB-T (multipleksi A i B) i DVB-T2 (multipleksi C i E), prikazani su vodoravnim linijama. Može se vidjeti da je, za relativno sličan omjer C/N, dobitak korisne brzine prijenosa oko 63% za DVB-T2, u odnosu na DVB-T sustav (22,4 Mbit/s za DVB-T u odnosu na 36,6 Mbit/s za DVB-T2).



**Slika 2.5.** Rezultati simulacije za DVB-T i DVB-T2 sustav sa sličnim parametrima odašiljanja kao u Hrvatskoj

#### 4.7. Zaključak

U ovom izvješću prikazali smo rezultate usporedbe DVB-T i DVB-T2 sustavima, sa tri različita modela kanala i sa sličnim parametrima odašiljanja kao u hrvatskim multipleksima. Ispitali smo Gaussov, Riceov i Rayleighev model kanala koji su definirani u ETSI normi. Rezultati pokazuju slične minimalne zahtijevane omjer C/N za Gaussov i Riceov model kanala, dok je za Rayleighev model kanala C/N omjer bio niži u simulaciji DVB-T2 sustava. Korisno povećanje brzine prijenosa bilo je oko 63%, kada se uspoređuju hrvatski DVB-T i DVB-T2 multipleksi (na nacionalnoj razini). Ovisno o korištenoj videokompresiji, zaključeno je da se može prenijeti 5-10 puta više kanala s istom vizualnom kvalitetom. Alternativno, mogli bi se implementirati HD i 3D kanali, kao što bi se dio frekvencijskog spektra mogao koristiti i za „drugu digitalnu dividendu“.

Prilikom usporedbe DVB-T i DVB-T2 sustava uz Gaussov kanal s istim parametrima odašiljanja koji se koriste u Hrvatskoj, minimalni omjer C/N je 17,2 dB za DVB-T sustav, dok je u DVB-T2 sustavu taj omjer bio 18,1 dB. Prilikom usporedbe Riceovog modela kanala, minimalni omjer C/N je bio 18,7 dB u DVB-T sustavu u odnosu na 18,6 dB za DVB-T2 sustav. Za Rayleighev model kanala, minimalni omjer C/N je 23 dB u DVB-T sustavu, u odnosu na 20,7 dB u DVB-T2 sustavu. To znači da se za modele kanala bez optičke vidljivosti mogu očekivati bolji rezultati u DVB-T2, nego u DVB-T sustavu, uz slične uvjete prijama.

Uz korištenje statističkog multipleksiranja i H.264/AVC videokompresije, može se zaključiti da je moguće emitiranje i do pet puta više TV kanala (s istom kvalitetom) u jednom

multipleksu DVB-T2 sustava u odnosu na DVB-T/MPEG-2 multipleks (kakav se koristi u Hrvatskoj). HEVC videokompresija je još uvijek u fazi razvoja, ali se može očekivati da će biti šire dostupna na tržištu za nekoliko godina. To će dodatno povećati broj TV programa koji se mogu emitirati, tako da bi bilo moguće i do 10 puta više TV programa u odnosu na trenutno emitiranje DVB-T/MPEG-2. Očekuje se da će HEVC kompresija udvostručiti stupanj kompresije podataka u odnosu na H.264/MPEG-4 AVC za istu kvalitetu videosignala. Alternativno, HD i 3D kanali bi mogli biti implementirani u DVB-T2 sustavu, kao što bi se neki frekvencijski spektar mogao koristiti za „drugu digitalnu dividendu“ (npr. za LTE).

Dodatnim poboljšanjima u OFDM sustavima s pomoću FTN prijenosa, DVB-T2 prijenos bi mogao biti dodatno poboljšan, u smislu povećanja korisne brzine prijenosa od 30-100% (u usporedbi s običnim OFDM) sa sličnim C/N, ali uz veći stupanj složenosti. Međutim, takve promjene treba izvesti na strani odašiljača i prijammnika te zahtijevaju daljnja istraživanja o implementaciji pilotskih podnosioca.

#### **4.8. Literatura**

- Vlada Republike Hrvatske, Strategija prelaska s analognog na digitalno emitiranje televizijskih programa u Republici Hrvatskoj, 2008.
- ETSI EN 300 744 V1.6.1, (2009-01): Digital Video Broadcasting (DVB); Framing structure, channel coding and modulation for digital terrestrial television
- ISO/IEC 13818-2: Information Technology - Generic Coding of moving pictures and associated audio information: Video, 1996.
- ETSI EN 300 421 V1.1.2 (1997-08): Digital Video Broadcasting; Framing structure, channel coding and modulation for 11/12 GHz satellite services
- EN 300 429 V1.2.1 (1998-04): Digital Video Broadcasting; Framing structure, channel coding and modulation for cable systems
- ISO/IEC 13818-1: Information technology - Generic coding of moving pictures and associated audio information: Systems, 1996.
- ITU-T Recommendation H.264 / ISO/IEC 14496-10: Information technology - Coding of audio-visual objects - Part 10: Advanced Video Coding, 2004.
- ITU-T Recommendation H.265 / ISO/IEC 23008-2 MPEG-H Part 2: Infrastructure of audiovisual services - Coding of moving video - High efficiency video coding, 2013.
- ETSI EN 302 307 V1.2.1 (2009-08): Digital Video Broadcasting (DVB); Second generation framing structure, channel coding and modulation systems for Broadcasting, Interactive Services, News Gathering and other broadband satellite applications (DVB-S2)
- ETSI EN 302 755 V1.1.1 (2009-09): Digital Video Broadcasting (DVB); Frame structure channel coding and modulation for a second generation digital terrestrial television broadcasting system (DVB-T2)
- ETSI EN 302 769 V1.1.1 (2010-04): Digital Video Broadcasting (DVB); Frame structure channel coding and modulation for a second generation digital transmission system for cable systems (DVB-C2)
- COM(2005) 204 final, Communication from the Commission to the Council, the European Parliament, the European Economic and Social committee and the Committee of the Regions on accelerating the transition from analogue to digital broadcasting, 2005.

- 
- DVB Fact Sheet: DVB-T2 - 2nd Generation Terrestrial Broadcasting, DVB Project Office, svibanj 2014.
- E. Dumić, S. Grgić, D. Frank, Simulating DVB-T to DVB-T2 Migration Opportunities in Croatian TV Broadcasting, Proceedings of 22nd International Conference on Software, Telecommunications and Computer Networks - SoftCOM 2014, rujanj 2014.
- M. Gosta, K. Šakić, „Digital dividend after the transition to DVB-T2“, Proc. of the 54th International Symposium ELMAR-2012, str. 243 – 246, rujanj 2012.
- I. Eizmendi et al, „DVB-T2: The Second Generation of Terrestrial Digital Video Broadcasting System“, IEEE Transactions on Broadcasting, Vol. 60, No. 2, str. 258 - 271, lipanj 2014.
- D. Dasalukunte, F. Rusek, J. B. Anderson, and V. Owall, „Design and Implementation of Iterative Decoder for Faster-than-Nyquist Signaling Multicarrier Systems“, IEEE Computer Society Annual Symposium on VLSI (ISVLSI), str. 359 - 360, srpanj 2011.
- J. B. Anderson, F. Rusek, V. Owall, „Faster-Than-Nyquist Signaling“, Proceedings of the IEEE, Vol. 101, No. 8, str. 1817 - 1830, kolovoz 2013.
- L. Polak, T. Kratochvil, „DVB-T and DVB-T2 performance in fixed terrestrial TV channels“, 35th International Conference on Telecommunications and Signal Processing (TSP), str. 725 - 729, srpanj 2012.
- M. Tormos et al, „Evaluation performance analysis of DVB-T2 in a SFN network“, 5th International Symposium on I/V Communications and Mobile Network (ISVC), str. 1-4, listopad 2010.
- E. Dumic, G. Sisul, S. Grgic, „Evaluation of Transmission Channel Models Based on Simulations and Measurements in Real Channels“, Frequenz, Vol. 66, No. 1-2, str. 41–54, veljača 2012.
- D. Tralic, E. Dumic, J. Vukovic, S. Grgic, „Simulation and Measurement of DVB-T2 System Parameters“, Proc. of the 54th International Symposium ELMAR-2012, str. 83 – 88, rujanj 2012.
- T. Richardson and R. Urbanke, „The Renaissance of Gallager's Low-Density Parity-Check Codes“, IEEE Commun. Magazine, vol. 41, str. 126-131, kolovoz 2003.
- D. Perez-Calderón, C. Oria, J. García, P. López, V. Baena, I. Lacadena, „Rotated Constellations for DVB-T2“, Proceedings of the 9th Conference on Design of Circuits and Integrated Systems (DCIS'09), Zaragoza (Spain), str. 41 – 45, studeni 2009.
- Envivio, „IP-based Statistical Rate Control“, dostupno na: [http://www.envivio.com/wp-content/uploads/2014/08/IPStatRate\\_Final.pdf](http://www.envivio.com/wp-content/uploads/2014/08/IPStatRate_Final.pdf), pristup, srpanj 2014.
- DVB-T2 Streams Parameter Sets, dostupno na [http://www.dvb.org/technology/dvbt2/DVB-T2\\_Streams\\_ParameterSets\\_SPLP.xls](http://www.dvb.org/technology/dvbt2/DVB-T2_Streams_ParameterSets_SPLP.xls), pristup: srpanj 2014.
- DVB-T2: The Common Simulation Platform, BBC R&D White Paper 196, dostupno na <http://downloads.bbc.co.uk/rd/pubs/whp/whp-pdf-files/WHP196.pdf>, pristup: srpanj 2014.
- EBU tech 3348, „Frequency and network planning aspects of DVB-T2“, version 3.0, studeni 2013.
-

## **5. Zaštita osobnih podataka u kontekstu pružanja usluga računarstva u oblaku prema pravu Europske unije i pravu Republike Hrvatske**

### **5.1. Sažetak**

Povod za ovo istraživanje recentni su razvojni momenti regulatorno-pravnog okvira Europske unije za zaštitu osobnih podataka u području pružanja usluga računarstva u oblaku (engl. *cloud computing*). Autori analiziraju i tumače relevantan pravni okvir Europske unije i Republike Hrvatske u pogledu niza aspekata obrade osobnih podataka u kontekstu pružanja usluga računarstva u oblaku. Do danas je velik dio regulatornih tijela država članica Europske unije tj. nadzornih tijela nadležnih za zaštitu osobnih podataka usvojio neke oblike smjernica i preporuka na temu zaštite osobnih podataka i *cloud computinga* (primjerice, u Njemačkoj, Sloveniji, Švedskoj, Italiji, Španjolskoj, Češkoj, Velikoj Britaniji, Francuskoj). Hrvatska agencija za zaštitu osobnih podataka izdala je takve smjernice 2012. godine i stoga ovo istraživanje uključuje i njihovu analizu. Autori također istražuju prijedlog novog regulatornog okvira Europske unije u općem području zaštite osobnih podataka, koji je trenutno u zakonodavnom postupku. To se istraživanje usredotočuje na odabrane odredbe najnovijeg nacrt teksta regulatornog okvira koji je usvojen od strane Europskog parlamenta, a kojim se mijenja izvorni prijedlog Europske komisije iz 2012. godine. Navedeni novi okvir značajno će utjecati na daljnji razvoj tržišta *cloud computing* usluga u Europskoj uniji pa tako i u Hrvatskoj. Autori zaključuju istraživanje procjenom mogućih utjecaja analiziranih rješenja za korisnike *cloud computing* usluga i pružatelje navedenih usluga te u odnosu na zakonodavstvo koje je trenutno na snazi. Istraživanje ima općenito za cilj doprinijeti podizanju svijesti javnosti o pravnim pitanjima zaštite osobnih podataka koja treba uzeti u obzir prilikom razmatranja prelaska u oblak, kao i razvoju domaće doktrine u ovome području.

## 5.2. Uvod

Prema široko korištenoj definiciji Nacionalnog instituta za standarde i tehnologije pri Ministarstvu trgovine Sjedinjenih Američkih Država (engl. *National Institute of Standards and Technology*, NIST) računarstvo u oblaku predstavlja model koji omogućava prikladan, sveprisutan mrežni pristup na zahtjev korisnika i to pristup zajedničkom skupu podesivih računalnih resursa (npr. mrežama, poslužiteljima, spremištima podataka, aplikacijama i uslugama), koji se mogu vrlo brzo pripremiti te staviti na raspolaganje uz minimalan upravljački napor, odnosno uz minimalno uzajamno djelovanje davatelja usluga. Ključne su osobine ovog modela usluga na zahtjev korisnika (samoposluživanje na zahtjev), široki spektar mogućnosti mrežnog pristupa, udruživanje resursa, brza elastičnost i tarifirana tj. mjerljiva usluga. Osnovni su modeli pružanja ove usluge softver kao usluga - SaaS, platforma kao usluga - PaaS, infrastruktura kao usluga - IaaS, dok se za kategorizaciju izvedbenih modela koriste pojmovi privatnog, zajedničkog, javnog i hibridnog oblaka. Opisana virtualizacija može pružiti niz prednosti za korisnike navedenih usluga, osobito u pogledu štednje uslijed moguće optimizacije njihovih poslovnih procesa bez potrebe ulaganja inače značajnih sredstava (ovisno o pojedinom modelu) u razvoj i održavanje relevantne infrastrukture kao i IT sustava.

2012. je godine Europska komisija usvojila strategiju *Oslobodimo potencijal cloud computinga* u Europi (tzv. *Cloud Computing* strategiju), u kojoj se utvrđuju mnoge društvene i ekonomske prednosti *cloud computinga* na razini EU-a, posebice kroz povećani rast BDP-a i otvaranje novih radnih mjesta. Kasnije je Komisija pokrenula i financijski podržala tzv. *Europsko Cloud partnerstvo* te uspostavu relevantnih standarda javne nabave. Osim toga, puno truda do danas uloženo je i u osiguravanje osnovnih tehničkih uvjeta i standardizaciju (interoperabilnost, prenosivost usluge). Dakako, često složena arhitektura *cloud computing* usluga i uvjeti njihovog pružanja otvaraju i niz drugih pitanja koja se trebaju riješiti, uključujući pitanje osiguravanja sigurnosti podataka u oblaku, a uvažavajući rizike povezane s virtualizacijom IT infrastrukture i sustava (u tom smislu mogu se istaknuti, na primjer, aktivnosti Europske agencije za sigurnost mreža i podataka (engl. *European Network and Information Security Agency*, ENISA).

Pri razmatranju pitanja primjene propisa na *cloud computing* okruženje treba uvodno napomenuti da se ovdje može primjenjivati čitav niz različitih pravnih područja, uključujući, ali ne ograničavajući se na područja informacijske sigurnosti i kibersigurnosti, zaštite potrošača, ugovornog prava i prava intelektualnog vlasništva, elektroničke trgovine, elektroničke identifikacije i povjerenja u elektroničke transakcije. U ovom istraživanju autori se usredotočuju isključivo na pravna pitanja koja su povezana s različitim aktivnostima tzv. obrade osobnih podataka u *cloud computingu*. Osobni podaci označavaju sve informacije koje se odnose na identificirane fizičke osobe ili fizičke osobe koje mogu biti identificirane (tzv. ispitanike), dok pojam obrade označava široki spektar aktivnosti koje se na te podatke mogu primijeniti (npr. prikupljanje, kopiranje, skladištenje, brisanje). Povod za istraživanje ovog pravnog područja leži osobito u činjenici da su se u tijeku javnih konzultacija koje su prethodile donošenju ranije spomenute *Cloud Computing* strategije upravo pitanja privatnosti i sigurnosti osobnih podataka nametnula kao jedna od temeljnih problematičnih pitanja.

Posebno se ističe kao problem nedostatna jasnoća u tumačenju i primjeni niza važnih aspekata *cloud computinga* u smislu propisa o zaštiti podataka, kao što su mjerodavno pravo, uloge različitih dionika (uključujući odgovarajuće odgovornosti i obveze) i prekogranični prijenos osobnih podataka. To se osobito ističe s obzirom na različita rješenja domaćih propisa država članica Europske unije, u kojima je implementirana Direktiva 95/46/EZ o zaštiti pojedinaca s obzirom na obradu osobnih podataka i o slobodnom kretanju takvih podataka (Opća direktiva). U svojoj strategiji Komisija stoga ukazuje i na postojeća tumačenja i smjernice stručnjaka u području zaštite osobnih podataka i računarstva u oblaku, poput onih koje je do sada izdalo neovisno savjetodavno tijelo EU-a osnovano prema čl. 29. Opće direktive (Radna skupina članka 29. o zaštiti pojedinaca s obzirom na obradu osobnih podataka, skraćeno: radna skupina članka 29.). To je tijelo, naime, 2012. godine donijelo mišljenje s detaljnim tumačenjima i preporukama oko praktične primjene važećeg EU okvira za zaštitu osobnih podataka (Opće direktive) u području *cloud computinga*, u kojem utvrđuje kao temeljni rizik nedostatak kontrole nad podacima te informacija oko njihove obrade. Autori analiziraju navedeno mišljenje u okviru istraživanja aktualnog pravno-regulatornog okvira EU-a.

Strategiju Europske komisije za rješavanje ranije navedenih problematičnih pitanja, s jedne strane rad čini rad na uspostavi modelnih ugovornih uvjeta korištenja usluga računarstva u oblaku, kojima bi se uredila pitanja kao što su zadržavanje podataka nakon prestanka ugovora, promjena usluge od strane pružatelja, podugovaranje, otkrivanje, lokacija, prijenos i integritet podataka te vlasništvo nad podacima. Posebice, Komisija predviđa da bi se ranije spomenuta problematična pitanja riješila kroz odgovarajuću primjenu budućeg novog općeg okvira zaštite osobnih podataka u EU (Opća uredba o zaštiti osobnih podataka). Danas je, naime, u tijeku zakonodavni postupak za donošenje tog novog okvira, koji bi trebao zamijeniti Opću direktivu. U ovom se istraživanju stoga detaljno analiziraju i odabrana relevantna rješenja iz prijedloga navedenog novog okvira. Razvojni momenti po pitanjima koja se istražuju na razini prava EU-a izravno utječu i na razvoj *cloud computing* tržišta u Republici Hrvatskoj i trebali bi se kao takvi razmatrati u kontekstu daljnjeg istraživanja tog područja u Hrvatskoj.

### **5.3. Istraživanje i rezultati**

#### **5.3.1. Važeći pravno-regulatorni okvir EU-a**

Prilikom tumačenja primjene važećeg pravnog okvira Europske unije u području zaštite osobnih podataka – Opće direktive treba imati na umu da je ova direktiva tehnološki neutralna i takva primjenjuje se također na obradu osobnih podataka u *cloud computing* okruženju. U području zaštite osobnih podataka temeljno je važno pravilno primijeniti koncepte tzv. voditelja zbirke osobnih podataka i izvršitelja obrade (terminologija hrvatskog Zakona o zaštiti osobnih podataka u kojem je implementirana Opća direktiva). Međutim, to može biti vrlo zahtjevan zadatak u modernim, složenijim uvjetima obrade podataka poput *cloud computinga*. Voditelj zbirke je, naime, onaj koji određuje (samostalno ili u suradnji s drugima) svrhu i način obrade ovih podataka i kao takav snosi temeljne obveze i odgovornosti za poštivanje propisa o zaštiti osobnih podataka. Prema tome, voditelj zbirke je prilikom obrade podataka dužan osigurati usklađenost s važećim propisima o zaštiti osobnih podataka,

što uključuje poštivanje niza propisanih obveza, poput provedbe odgovarajućih mjera njihove zaštite od svake neovlaštene obrade. Također je dužan osigurati ispunjenje temeljnih zahtjeva koje nalažu relevantni propisi (npr. zahtjev da se osobni podaci obrađuju pošteno i zakonito, prikupljaju u svrhu s kojom je ispitanik upoznat, koja je izričito navedena i u skladu sa zakonom i da se dalje obrađuju samo u svrhu u koju su prikupljeni, odnosno u svrhu koja je podudarna sa svrhom prikupljanja, da podaci budu bitni za postizanje utvrđene svrhe i da se ne prikupljaju u većem opsegu nego što je to nužno da bi se postigla utvrđena svrha te da se čuvaju u obliku koji dopušta identifikaciju ispitanika ne duže no što je to potrebno za svrhu u koju se podaci prikupljaju ili dalje obrađuju i dr.). Voditelji zbirke moraju se jasno razlikovati od izvršitelja obrade, koji po nalogu i sukladno uputama voditelja samo obavljaju one poslove obrade osobnih podataka koje im je voditelj zbirke povjerio. Prema tome, u skladu s navedenom podjelom uloga u području zaštite podataka prema Općoj direktivi, voditelji zbirke temeljno su odgovorni za usklađeno postupanje s mjerodavnim propisima o zaštiti osobnih podataka, dok izvršitelji obrade, koji vrše obradu u njihovo ime, imaju tek ograničene obveze.

Utvrđivanje uloga voditelja zbirke i izvršitelja obrade potrebno je provoditi za svaki pojedini slučaj kako bi se, primjerice, utvrdio stupanj kontrole svakog od njih nad obradom osobnih podataka u pitanju. Ranije smo napomenuli da to može predstavljati izazov osobito u modernim uvjetima pružanja složenijih *cloud computing* sustava, a koji obuhvaćaju više različitih arhitektonskih slojeva, budući da razina kontrole nad uključenom obradom podataka može značajno varirati (na primjer, tamo gdje pružanje *cloud computing* usluga uključuje nekoliko različitih stadija obrade podataka). Osim toga smatra se da bi u nekim slučajevima, kao što su isključiva infrastrukturna *cloud* rješenja, a s obzirom na zanemariv stupanj kontrole nad uključenom obradom podataka, pružatelji tih usluga mogli imati i sasvim neutralnu - posredničku ulogu u smislu propisa o zaštiti osobnih podataka. U svojem mišljenju na temu zaštite osobnih podataka u kontekstu *cloud computinga* radna skupina članka 29. utvrdila je postojanje mogućnosti da se u određenim slučajevima pružatelji *cloud* usluga smatraju zajedničkim voditeljima zbirke osobnih podataka (zajedno s korisnicima tih usluga), a ne pukim izvršiteljima obrade prema tradicionalnom modelu raspodjele uloga i odgovornosti iz Opće direktive), ili čak zasebnim voditeljima (npr. ako obrađuju osobne podatke za svoje potrebe). Štoviše, u nekim slučajevima, kao što su to *cloud* usluge društvenih mreža, smatra se da će pružatelji tih usluga preuzeti ulogu voditelja relevantnih zbirke osobnih podataka, jer su oni ti koji određuju svrhu i način njihove obrade (podaci koje krajnji korisnici objavljuju i razmjenjuju s drugima). Uz navedene ograde navedeno se mišljenje radne skupine članka 29. ipak ponajviše temelji na tumačenju tradicionalnog modela, prema kojem se pružatelji *cloud* usluga smatraju izvršiteljima obrade osobnih podataka koji ih obrađuju u ime korisnika tih usluga. U takvim je slučajevima korisnik usluge u ulozi voditelja zbirke dužan osigurati poštovanje relevantnih propisa, odnosno korisnik snosi temeljnu odgovornost za postupanje u skladu s važećim propisima o zaštiti podataka. To se odnosi i na slučajeve kada se od korisnika traži da prihvati pružateljeve standardizirane uvjete korištenja u pogledu obrade osobnih podataka. Drugim riječima, korisnici nisu samo zbog toga što ne sklapaju zaseban, individualizirani ugovor o obradi podataka s pružateljem *cloud* usluga oslobođeni svojih obveza osiguravanja usklađene obrade osobnih podataka s važećim propisima. Stoga oni



prilikom ugovaranja *cloud* usluga moraju izabrati samo one pružatelje *cloud* usluga koji jamče poštivanje tih pravila. U tu svrhu utvrđuje se niz korisnih detalja o sadržaju ugovornog odnosa između pružatelja *cloud* usluga i korisnika, u kojem se osobito mora zadovoljiti načelo transparentnosti prema korisniku što se tiče namjeravane obrade osobnih podataka. Osim toga utvrđuje se i niz posebnih obveza za slučajeve kada pružatelji usluga žele angažirati podizvođača za obavljanje pojedinih poslova obrade osobnih podataka (prethodna privola korisnika, sklapanje ugovora s obveznim sadržajem) i kada se obrada podataka obavlja na različitim lokacijama, uključujući osobito slučaj njihovog prijenosa u treće zemlje tj. izvan EU-a).

### 5.3.2. Analiza važećeg pravnog okvira Republike Hrvatske i aktivnosti nadzornog tijela u području zaštite osobnih podataka i *cloud computinga*

U analizi domaćeg pravno-regulatornog okvira zaštite osobnih podataka istražuju se rješenja važećeg Zakona o zaštiti osobnih podataka u odnosu na *cloud computing* okruženje i u odnosu na Opću direktivu koja je provedena u domaći pravni okvir kroz navedeni zakon. Analiziraju se i specifičnosti domaćeg okvira, poput posebnih obveza kod obrade posebno osjetljivih osobnih podataka - *posebne kategorije osobnih podataka*, kao što su to npr. podaci o zdravlju, a kada je potrebno pridržavati se i *Uredbe Vlade RH o načinu pohranjivanja i posebnim mjerama tehničke zaštite posebnih kategorija osobnih podataka* iz 2004. godine. Za obradu osobnih podataka u *cloud computing* uvjetima posebno su važne smjernice (preporuke) Agencije za zaštitu osobnih podataka iz 2012. godine. Iz navedenih smjernica može se zaključiti da prilikom utvrđivanja uloga i odgovarajućih odgovornosti zaštite osobnih podataka Agencija uglavnom smatra pružatelje *cloud* usluga izvršiteljima obrade, a njihove klijente (korisnike usluga) voditeljima zbirki. Analiza navedenih smjernica obuhvaća između ostalog ispitivanje obveza i posebnih preporuka prilikom ugovaranja *cloud computing* usluga, uključujući upozorenja oko specifičnih rizika te obveze implementacije odgovarajućih mjera zaštite, ali i preporuke za provedbu standarda informacijske sigurnosti (npr. ISO 27001), revizijskih mjera i dr.

### 5.3.3. Ispitivanje predloženih rješenja budućeg općeg okvira EU-a za zaštitu osobnih podataka u *cloud* okruženju

Konačni dio istraživanja obuhvaća opsežan prijedlog novog pravno-regulatornog okvira - Opće uredbe i to onih aspekata za koje autori ocjenjuju da najviše utječu na pitanja pružanja usluga računarstva u oblaku unutar Europske unije koja su predmet ovog istraživanja. Autori usporedno ispituju rješenja izvornog prijedloga rješenja Europske komisije iz 2012. godine u odnosu na nacrt teksta s izmjenama i dopunama navedenog, a kojeg je nedavno (ožujak 2014.) usvojio Europski parlament. Ta analiza ukazuje na niz značajnih pomaka u svrhu utvrđivanja preciznosti novih pravila za sve *cloud computing* dionike u svim državama članicama EU-a. Tome je razlog osobito predložena vrsta pravnog instrumenta za donošenje navedenih novih pravila (uredba), jer su uredbe u pravu Europske unije, za razliku od direktiva, obvezujuće u cijelosti i izravno se primjenjuju u svim državama članicama. Opća uredba o zaštiti osobnih podataka zamijenila bi, naime, dosadašnju Opću direktivu, a čija je provedba, kako smo ranije napomenuli, obilježena problematikom različitih nacionalnih rješenja u državama članicama EU-a i to osobito dolazi do izražaja prilikom njihove primjene

na slučajevne obrade podataka u oblaku. Potreba uspostave što učinkovitijeg novog pravnog okvira očituje se i u prijedlogu značajno ojačanih ovlasti nadležnih nadzornih tijela za zaštitu osobnih podataka, poput novouvedene ovlasti izravnog sankcioniranja povreda. U određenim bi slučajevima tako ova tijela bila ovlaštena izreći novčane kazne u iznosu do čak 100 000 000 EUR, odnosno do 5% godišnjeg bruto domaćeg proizvoda (tvrtke), ovisno o tome koji je od ta dva iznosa veći. Neka od novih i/ili poboljšanih rješenja u odnosu na trenutno važeću Opću direktivu, a koje autori izdvajaju za svrhu ovog izvješća, jesu kako slijedi. Autori ocjenjuju da će predložena rješenja novog okvira EU-a značajno olakšati postupke osiguravanja usklađenosti postupanja kod obrade podataka osobito za one pružatelje *cloud* usluga koji pružaju svoje usluge (tj. u tom kontekstu provode obradu osobnih podataka) u više država članica EU-a. Osim toga, autori ocjenjuju da daljnja važna korist za pružatelje *cloud* usluga leži u predloženom rješenju da njihove relevantne aktivnosti obrade podataka u svim državama članicama budu pod nadzorom jednog tijela - nadzornog tijela njihovog glavnog poslovnog nastana. Nadalje ocjenjuju da će se zaštita korisnika *cloud computing* usluga u EU-u značajno učinkovitije nego do sada provoditi i uslijed predloženog širokog teritorijalnog opsega Opće uredbe. Ona bi se, naime, pod određenim uvjetima primjenjivala i na pružatelje *cloud* usluga izvan EU-a.

Što se tiče analize novih rješenja temeljnih koncepata zaštite osobnih podataka, autori izdvajaju prijedlog proširene definicije osobnih podataka radi uključivanja identifikatora kao što su podaci o lokaciji i jedinstveni identifikatori (to bi u određenim slučajevima moglo uključivati i identifikatore poput IP adresa, identifikatora kolačića, RFID-a i sl.).

Nacrt Opće uredbe ima za cilj jasnije podijeliti odgovornosti i obveze svih onih koji su učinkovito zaduženi za obradu podataka, što je posebno važno u složenijim uvjetima obrade podataka poput *cloud computinga*. Osim toga potrebno je jasnije nego sada utvrditi i situacije kao što je obrada osobnih podataka koju zajednički provodi više voditelja zbirke osobnih podataka. U tom smislu ističu se i stavovi pojedinih važnih tijela EU-a, posebno u odnosu na nacrt Opće uredbe u kontekstu *Cloud Computing* strategije Europske komisije, a prema kojima se u nizu slučajeva pružatelji *cloud* usluga trebaju smatrati zajedničkim voditeljima zbirke osobnih podataka ili suvoditeljima - zajedno s korisnicima tih usluga. Navedeno se smatra posebno opravdanim u slučajevima kada korisnici *cloud* usluga imaju vrlo ograničenu razinu kontrole nad sredstvima za obradu podataka, odnosno vrstom usluge koja im se nudi (npr. kod SaaS rješenja za uredsku učinkovitost i poslovnu inteligenciju.) U takvim slučajevima trebalo bi, dakle, primijeniti nova rješenja Opće uredbe u svrhu međusobnog uređenja obveza zaštite osobnih podataka više voditelja zbirke osobnih podataka, pitanja zajedničke obrade podataka i poštivanja svih obveza koje se na njih odnose. Jasnije pripisivanje odgovornosti za sve one koji su zaduženi za obradu podataka također je rezultiralo opsežnijim tj. detaljnijim uređenjem obveza i odgovornosti kod povjeravanja poslova obrade podataka (voditelj zbirke - izvršitelj obrade) i zaštite podataka. Za slučajeve kada se primjenjuje „tradicionalan“ odnos uloga (voditelj zbirke – izvršitelj obrade), ističu se rješenja kojima se uređuje značajno više detalja međusobnog odnosa navedenih dionika nego što je to trenutno uređeno Općom direktivom.

Za svrhu ovog izvješća autori ističu i to da Opća uredba (kao i dosadašnja Opća direktiva) potiče razvoj tzv. *kodeksa ponašanja* u svrhu konkretne primjene novih rješenja u pojedinim sektorima, kao što je to sektor *cloud computinga*. S time u vezi ukazuju i na nužnost praćenja aktualnosti oko predloženog kodeksa ponašanja za pružatelje *cloud* usluga (*Cloud Select Industry Group on Code of Conduct*) koji bi se primjenjivao na razini EU-a i koji je stoga podnesen na odobrenje radnoj skupini članka 29.

Daljnja važna novouvedena dužnost u kontekstu *cloud computinga*, kako za voditelje zbirke tako i izvršitelje obrade, primjena je tehničkih i organizacijskih mjera i postupaka koji su potrebni kako bi se osigurala obrada osobnih podataka koja je u skladu s Uredbom - tijekom cjelokupnog životnog vijeka podataka. Postroženo načelo transparentnosti kod obrade osobnih podataka uključuje izričitu obvezu obavještanja u slučajevima namjeravanog prekograničnog prijenosa osobnih podataka. Također je vrlo važno uređenje postupaka izvješćivanja o povredama osobnih podataka. Navedeno se, dakako, primjenjuje i u *cloud computing* kontekstu te se mora na odgovarajući način regulirati kako u odnosima gdje postoji više zajedničkih voditelja zbirke osobnih podataka (pružatelj *cloud* usluge, korisnik) tako i u „tradicionalnim“ odnosima gdje se korisnik smatra voditeljem zbirke, a pružatelj usluge izvršiteljem obrade. Svakako, naglašena rješenja Opće uredbe na prvome su mjestu prijedlozi postroženih obveza i odgovornosti voditelja zbirke, međutim, izvršiteljima obrade također bi se pripisala brojna nova zaduženja, kao i utvrdila njihova izravna odgovornost prema ispitanicima i regulatornim tijelima.

#### **5.4. Zaključak**

Iako danas još uvijek nije jasno hoće li novi opći okvir zaštite osobnih podataka EU-a konačno biti usvojen u obliku uredbe koja bi se izravno primjenjivala u svim državama članicama (kao i konačna rješenja novog okvira), činjenica jest da je Komisija u svojoj *Cloud Computing* strategiji naglasila nužnost što bržeg usvajanja novih, što jasnijih rješenja radi rješavanja pravne nesigurnosti po nizu pitanja zaštite podataka u *cloud computing* okruženju, a koja su u dijelu uzrokovana i različitim nacionalnim rješenjima u tom području. Iako je vjerojatno da novi pravno-regulatorni okvir neće dati jednoznačne odgovore na baš sva pitanja koja se specifično javljaju kod obrade osobnih podataka u oblaku, tome će svakako doprinijeti snažna podrška izradi kodeksa ponašanja za ovaj sektor (kao što je to i ranije navedeni kodeks koji je predan radnoj skupini članka 29. na odobrenje). Osim toga, neka od gorućih pitanja moguće je razjasniti i putem preporuka, smjernica i najbolje prakse koje bi donosilo tijelo koje će zamijeniti današnju radnu skupinu članka 29. (Europski odbor za zaštitu podataka). Konačno, sama Komisija bi prema nacrtu Opće uredbe trebala dobiti ovlaštenje za usvajanje delegiranih akata u određenim područjima pa tako vjerujemo i u području obrade i zaštite osobnih podataka u oblaku.

U Hrvatskoj, koja je implementirala danas još uvijek važeću Opću direktivu u Zakonu o zaštiti osobnih podataka, smjernice o zaštiti podataka i *cloud computingu* koje je donijela Agencija za zaštitu osobnih podataka trebale bi se promicati među svim dionicima, ali i u široj javnosti. Sve aktualnosti u vezi s novim pravno-regulatornim režimom zaštite podataka na

razini EU-a trebaju se pomno pratiti kako bi se već sada razmatrao njihov utjecaj u *cloud* kontekstu (npr. strože odgovornosti i brojne nove i/ili postrožene obveze voditelja zbirki ali i izvršitelja obrade, te specifičnosti oko uređenja ugovornih odnosa između navedenih dionika). Ovime se također omogućuje pravovremena procjena prilagodbe postojećih politika zaštite osobnih podataka i postojećih ugovornih odnosa (pružatelj *cloud* usluge – korisnik, pružatelji *cloud* usluga i njihovi podizvođači i dr.). Osobito je važno već danas razmatrati pravilnu primjenu propisa o zaštiti osobnih podataka na one *cloud* modele koji mogu zahtijevati drugačiju raspodjelu uloga i odgovornosti nego što je to karakteristično za tradicionalne modele obrade podataka, kao što su to osobito oni gdje su pružatelji *cloud* usluga zajednički voditelji zbirki osobnih podataka s korisnicima usluga i sl. Osobito u *cloud* okruženju dolazi do potrebe jačanja svijesti o raspoloživim pravnim mehanizmima za prijenose podataka izvan EU-a i u tom je pogledu također nužno redovito praćenje aktualnosti unutar EU-a po ovim pitanjima. Primjer toga između ostalog je i nedavno odobrenje Microsoftovih uvjeta pružanja *cloud* usluga za poduzeća u kontekstu međunarodnog prijenosa osobnih podataka od strane radne skupine članka 29., kojim se utvrdila usklađenost tih uvjeta sa zahtjevima za međunarodnim prijenos podataka sukladno standardnim ugovornim klauzulama EU-a. Nije nužno posebno naglašavati i potrebu redovitog konzultiranja izdanih dokumenata i preporuka na temu zaštite podataka i *cloud computinga*, npr. od strane radne skupine članka 29. (čiji je aktivan član i Agencija za zaštitu osobnih podataka) te europskog nadzornika zaštite podataka. Autori smatraju da bi sve navedene informacije trebale biti transparentne i lako dostupne za hrvatsku javnost, na primjer na internetskim stranicama Agencije za zaštitu osobnih podataka i to po mogućnosti u okviru teme isključivo posvećenoj zaštiti podataka i računarstvu u oblaku.

Autori smatraju da bi svi navedeni koraci značajno pridonijeli prijeko potrebnom podizanju svijesti javnosti na temu zaštite podataka i *cloud computinga* te pomogli korisnicima i pružateljima *cloud* usluga u Republici Hrvatskoj da na odgovarajući način riješe otvorena pitanja i procijene svoju relevantnu praksu. Sve je jasnije da osiguravanje i promicanje odgovarajuće prakse zaštite privatnosti i osobnih podataka na globalnom *cloud computing* tržištu može predstavljati konkurentsku prednost između različitih pružatelja usluga. Autori stoga smatraju poželjnim uzimanje u obzir (daljnjeg) povećanja transparentnosti *cloud* rješenja i uvjeta zaštite podataka od strane domaćih pružatelja *cloud* usluga, npr. pojašnjenjem prakse zaštite privatnosti i sigurnosti te uvjeta pružanja usluga na njihovim internetskim stranicama, a čime bi se ujedno promicala dodatna vrijednost tih rješenja prema svim potencijalnim korisnicima.

## 5.5. Literatura

[1] National Institute of Standards and Technology, „NIST Special Publication 800-145 - The NIST Definition of Cloud Computing“, September 2011, <http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf>.

[2] „Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Unleashing the Potential of Cloud Computing in Europe“, Brussels, 27.9.2012, COM(2012) 529 final.

[3] ENISA, „Cloud computing - benefits, risks and risk assessment for information security“, 20.11. 2009; „Cloud computing - information assurance framework“, 20.11.2009, „Security & resilience in Governmental clouds – making an informed decision“, 17.11.2011, „Procure secure: a guide to monitoring of security service levels in cloud contracts“, 02.04.2012, „Auditing security measures - an overview of schemes for auditing security measures“, 03.10.2013, „Good practice guide for securely deploying Governmental clouds“, 15.11.2013, „Certification in the EU Cloud Strategy“, 12.11.2013, „Cloud security incident reporting - framework for reporting about major cloud security incidents“, 09.12.2013. Sve dostupno na: <http://www.enisa.europa.eu/>.

[4] „Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data“, Službeni list Europske unije L 281, 23. 11. 1995, str. 31–50.

[5] European Commission, „Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)“, COM (2012) 11 final, 2012/0011 (COD), Brussels, 25.1.2012.

[6] Article 29 Data Protection Working Party, „Opinion 05/2012 on cloud computing“, 01037/12/EN, WP 196, 01.7.2012.

[7] I. Lovrek, T. Lovrić, D. Lučić, „Regulatory aspects of cloud computing“, Proceedings SoftCOM 2012 International Conference on Software, Telecommunications and Computer Networks, Workshop on Regulatory Challenges, Split, Croatia, 2012; N. Gumzej, „Protection of Data Relating to EU Consumers in the IoT Age“, Proceedings SoftCOM 2012 International Conference on Software, Telecommunications and Computer Networks, Workshop on Regulatory Challenges, Split, Croatia, 2012; N. Gumzej, „Selected Legal Aspects of Cloud Computing Services“, Conference Proceedings CASE 24 – Development of Business and Information Systems, Zagreb, Croatia, 2012.

[8] W. K. Hon, E. Kosta, C. Millard, D. Stefanatou, „Cloud accountability: the likely impact of the proposed EU Data Protection Regulation“, Queen Mary School of Law Legal Studies Research Paper No. 172/2014; Tilburg Law School Research Paper No. 07/2014, <http://ssrn.com/abstract=2405971>; W. K. Hon, C. Millard, I. Walden, „Who is responsible for ‘personal data’ in cloud computing?—The cloud of unknowing“, Part 2 (21.3.2011), International Data Privacy Law, 2012, Vol. 2, broj 1, str. 3-18; Queen Mary School of Law Legal Studies Research Paper No. 77/2011, <http://ssrn.com/abstract=1794130>.

[9] C. Gayrel, J. Gérard, J.-P. Moïny, Y. Pouillet, J.-M. Van Gysegheem, „Cloud computing and its implications on data protection“, discussion paper for Council of Europe Project on Cybercrime, Namur, Belgium, 05.3.2010, <http://www.coe.int/t/dghl/cooperation/>

economiccrime/cybercrime/Documents/Reports-Presentations/2079\_reps\_IF10\_yvespoulet1 b.pdf; Y. Poulet, J.-M. Van Gyseghem, J.-P. Moïny, J. Gérard, C. Gayrel, „Data protection in the clouds“, in *Computers, Privacy and Data Protection: an Element of Choice*, S. Gutwirth, Y. Poulet, P. De Hert, R. Leenes, Eds., str. 377-409.

[10] W. K. Hon, E. Kosta, C. Millard, D. Stefanatou, „Cloud accountability: the likely impact of the proposed EU Data Protection Regulation“, Queen Mary School of Law Legal Studies Research Paper No. 172/2014; Tilburg Law School Research Paper No. 07/2014, SSRN: <http://ssrn.com/abstract=2405971>; P. De Hert, V. Papakonstantinou, „The proposed data protection regulation replacing Directive 95/46/EC: a sound system for the protection of individuals“, *Computer Law & Security Review*, vol. 28, broj 2, 2012, str. 130 – 142; I. S. Nwankwo, „Missing links in the proposed EU Data Protection Regulation and cloud computing scenarios: a brief overview“, *Journal of Intellectual Property, Information Technology and E-Commerce Law*, vol. 5, broj 1, 2014, str. 32-38, [https://www.jipitec.eu/issues/jipitec-5-1-2014/3905/jipitec\\_5\\_1\\_nwanko.pdf](https://www.jipitec.eu/issues/jipitec-5-1-2014/3905/jipitec_5_1_nwanko.pdf).

[11] European Commission, „Commission decisions on the adequacy of the protection of personal data in third countries“, [http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index\\_en.htm#h2-14](http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm#h2-14).

[12] European Commission, „Model contracts for the transfer of personal data to third countries“, [http://ec.europa.eu/justice/data-protection/document/international-transfers/transfer/index\\_en.htm](http://ec.europa.eu/justice/data-protection/document/international-transfers/transfer/index_en.htm).

[13] European Commission, „Overview on binding corporate rules“, [http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/index\\_en.htm](http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/index_en.htm).

[14] European Commission, „Commission decisions on the adequacy of the protection of personal data in third countries – US - United States - Safe Harbor“, [http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index\\_en.htm#h2-14](http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm#h2-14).

[15] European Commission, „Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council“, *Službeni list Europske unije* L 39, 12.2.2010, str. 5-18.

[16] Article 29 Data Protection Working Party, „Letter to Microsoft, Ref. Ares(2014)1033670 - 02/04/2014“, Brussels, 02.4.2014, [http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140402\\_microsoft.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140402_microsoft.pdf).

[17] Zakon o zaštiti osobnih podataka, *Narodne novine* br. 103/03, 118/06, 41/08, 130/11 – 106/12 – pročišćeni tekst.

[18] Uredba o načinu pohranjivanja i posebnim mjerama tehničke zaštite posebnih kategorija osobnih podataka, *Narodne novine* br. 139/04.

[19] Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, „Orientierungshilfe – Cloud Computing“, 26.9.2011, [http://www.bfdi.bund.de/DE/Themen/TechnologischerDatenschutz/TechnologischeOrientierungshilfen/Artikel/OHCloudComputing.pdf?\\_\\_blob=publicationFile](http://www.bfdi.bund.de/DE/Themen/TechnologischerDatenschutz/TechnologischeOrientierungshilfen/Artikel/OHCloudComputing.pdf?__blob=publicationFile); Information Commissioner, „Personal data protection & cloud computing“, 15.6.2012, [https://www.ip-rs.si/fileadmin/user\\_upload/Pdf/smernice/Cloud\\_computing\\_and\\_data\\_protection\\_-\\_ENG\\_final.pdf](https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Cloud_computing_and_data_protection_-_ENG_final.pdf); Datainspektionen, „Cloud services and the Personal Data Act“, <http://www.datainspektionen.se/Documents/faktablad-cloudservices.pdf>; Úřad pro ochranu osobních údajů, „K právní ochraně osobních údajů při jejich předávání v rámci cloudových služeb“, 27.8.2013, [http://www.uouu.cz/VismoOnline\\_Action\\_Scripts/File.ashx?id\\_org=200144&id\\_dokumenty=3002](http://www.uouu.cz/VismoOnline_Action_Scripts/File.ashx?id_org=200144&id_dokumenty=3002); Il Garante per la protezione dei dati personali, „Cloud computing - how to protect your data without falling from a cloud“, <http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1906139>; Agencia Española de Protección de Datos, „Guía para clientes que contraten servicios de cloud computing“, 2013, [http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA\\_Cloud.pdf](http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_Cloud.pdf); „Orientaciones para prestadores de servicios de cloud computing“, 2013, [http://www.agpd.es/portalwebagpd/canaldocumentacion/publicaciones/common/guias/orientaciones\\_cloud.pdf](http://www.agpd.es/portalwebagpd/canaldocumentacion/publicaciones/common/guias/orientaciones_cloud.pdf); Information Commissioner's Office, „Guidance on the use of cloud computing“, 2012, [http://ico.org.uk/for\\_organisations/data\\_protection/topic\\_guides/online/cloud\\_computing](http://ico.org.uk/for_organisations/data_protection/topic_guides/online/cloud_computing); La Commission Nationale de l'Informatique et des Libertés, „Cloud computing: les conseils de la CNIL pour les entreprises qui utilisent ces nouveaux services“, 25.6.2012, <http://www.cnil.fr/linstitution/actualite/article/article/cloud-computing-les-conseils-de-la-cnil-pour-les-entreprises-qui-utilisent-ces-nouveaux-services/>.

[20] S. Grgić, Agencija za zaštitu osobnih podataka, „ISO 27001 zaštita osobnih podataka i računalstvo u oblaku“, 2012.

[21] „Opinion of the European Data Protection Supervisor on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe"“, Brussels, 16.11. 2012, [https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2012/12-11-16\\_Cloud\\_Computing\\_EN.pdf](https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2012/12-11-16_Cloud_Computing_EN.pdf).

[22] P. De Hert, V. Papakonstantinou, „The proposed data protection regulation replacing Directive 95/46/EC: a sound system for the protection of individuals“, Computer Law & Security Review, vol. 28, broj 2, 2012.

[23] European Commission, Digital Agenda for Europe, Telecoms and the Internet, Cloud Computing, European Strategy, Working Groups, „The Cloud Select Industry Group on Code of Conduct“, <https://ec.europa.eu/digital-agenda/en/cloud-select-industry-group-code-conduct>; European Commission, Press releases, “New guidelines to help EU businesses use the Cloud”, IP/14/743, Brussels, 26.6.2014, [http://europa.eu/rapid/press-release\\_IP-14-743\\_en.htm](http://europa.eu/rapid/press-release_IP-14-743_en.htm).

## 6. Regulatorna perspektiva buduće komunikacijske mreže i Interneta

### 6.1. Uvod

Sadašnje komunikacijske mreže, uključujući i Internet, suočene su s novim komunikacijskim uzorcima koji proizlaze prvenstveno iz umrežavanja sadržaja i društvenog umrežavanja te mobilnosti i sigurnosti, a koji traže velike kapacitete i adekvatne performanse. Stoga su nova rješenja za umrežavanje predmet intenzivnih istraživanja. Primjerice, radni okvir buduće mreže (engl. *Future Network*, FN) Međunarodne telekomunikacijske unije (engl. *International Telecommunication Union*, ITU) bavi se nedovoljno razrađenim pitanjima današnjih mreža i mogućnostima koje trebaju otvoriti buduće mreže. Ključna su istraživanja vezana uz sveprisutni pristup i pokretljivost, sigurnost i povjerenje, performanse te paradigme usmjerene sadržaju i računarstvu. Mnoga tehnička i netehnička pitanja podudaraju se s onima koja obuhvaća istraživačko područje budućeg Interneta (engl. *Future Internet*, FI).

S regulatornog motrišta treba razmatrati četiri dimenzije: tržišnu, gospodarsku, društvenu i javnu, kad je riječ o budućoj mreži i Internetu. Glavna razlika između „sadašnjeg“ i „budućeg“ je u tome što današnje mreže i Internet nisu oblikovani uz takve pretpostavke, tj. ne obuhvaćaju tehnička i netehnička rješenja koja proizlaze iz novih zahtjeva. Stoga su u današnjim mrežama i Internetu nužna posebna rješenja koja se uvode u arhitekturu i funkcionalnost, kako bi se odgovorilo svakom pojedinom zahtjevu. Informacijska sigurnost je najbolji primjer za to.

Elektroničke komunikacije izložene su tako dinamičnom razvoju da je razlikovanje „sadašnjeg“ i „novog“ ili „novog“ i budućeg“ u mnogim slučajevima praktički nemoguće. Dobra su ilustracija za to Internet stvari (engl. *Internet of Things*, IoT), komunikacija strojeva (engl. *Machine-to-Machine communication*, M2M) i računarstvo u oblaku (engl. *cloud computing*) koji će se u nastavku posebno obraditi. Rasprava društvenih i gospodarskih aspekata vezana uz elektroničke komunikacije nužno vodi prema pitanjima Digitalne agende za Hrvatsku.

Dosadašnja iskustva u istraživanju i razvoju komunikacijskih mreža i sustava, informacijske i komunikacijske tehnologije (engl. *Information and Communication Technology*, ICT) te regulatornih iskustava sažimaju se u izvornom prijedlogu i novom modelu regulatornog prostora koji može odgovoriti izazovima budućih mreža i budućeg Interneta.

### 6.2. Istraživanja u području budućih mreža

Interdisciplinarna istraživanja u području budućih mreža obuhvaćaju različite poglede na elektroničke komunikacije i primjenu informacijske i komunikacijske tehnologije. „*Future Network*“ predočuje radni okvir ITU-T-a [1]. „*Future Internet*“ je izraz sadržan u mnogim inicijativama, programima i projektima u svijetu [2, 3], a samo Sedmi okvirni program Europske unije (EU FP7) obuhvatio je oko 150 projekata na tu temu [4, 5].



ITU-T je definirao četiri cilja za FN: a) svjesnost o uslugama, b) svjesnost o podacima, c) svjesnost o okolišu, i d) društvena i gospodarska svjesnost, što ukazuje na temeljnu razliku današnje i buduće mreže [6].

Očekivana raznolikost usluga za stacionarne i pokretne korisnike (osobe i strojeve) zahtijeva fleksibilnu funkcionalnost, neograničenu pokretljivost, sigurnost i pouzdanost za kritične usluge, drugim riječima svjesnost o uslugama koje se pružaju korisnicima. Raznolikost usluga nije samo budući, već i sadašnji zahtjev koji proizlazi iz sve veće komunikacije strojeva putem pokretne mreže.

Svjesnost o podacima povezana je s načinom kojim se uspostavlja komunikacija i izmjenjuju podaci. Postojeće usmjeravanje između krajnjih točaka zasnovano je na lokaciji, s jedinstvenom globalnom identifikacijom lokacije. Kad i ako isti identifikator označava višestruke istovrsne sadržaje, javlja se problem optimalnog usmjeravanja do najbližeg sadržaja. Usmjeravanje i s njim povezano rukovanje identifikatorima koje na ovaj način uzima u obzir sadržaj otvoreno je pitanje. Ponovno se otvara i pitanje inteligencije mreže.

Buduće mrežne arhitekture i tehnologije trebaju imati pozitivan utjecaj na okoliš, kao i društvo i gospodarstvo u cijelosti. Svjesnost o okolišu u najmanju ruku se podudara s općim zahtjevom za smanjenjem emisije ugljičnog dioksida. Komunikacijske mreže već su postale društvena infrastruktura, a njihova društvena uloga bit će sve veća. Isto vrijedi za gospodarstvo i poslovne aktivnosti u ICT-sektoru i sektoru elektroničkih komunikacija, kao i u svim ostalima.

Transformacija današnjih mreža sukladno konceptu mreže sljedeće generacije (engl. *Next Generation Network*, NGN) koja je u tijeku i u Hrvatskoj, već slijedi neke od navedenih ciljeva, primjerice pozicioniranje usluga u uslužni stratum („svjesnost o uslugama“), s ograničenjima koja proizlaze iz arhitekture IP-mreže s mrežnim protokolom IPv4. Međutim treba upozoriti da funkcije za potporu izmjene i obrade sadržaja nisu uključene u NGN [7].

Istraživačka domena „*Future Internet*“ isto tako bavi se različitim tehničkim i netehničkim pitanjima usmjerenima na unaprjeđenja ili nova načela umrežavanja [8]. Kao što je već rečeno, ključni su sveprisutni pristup i pokretljivost, sigurnost i povjerenje, usmjerenost sadržaju i računarstvu. Međutim, i ovdje se budućnost ubrzano približava u dijelovima kao što su IoT i računarstvo u oblaku. Svakako treba uočiti da je pokretljivost u današnjem Internetu moguće riješiti, dok se problemi sigurnosti mogu samo smanjiti.

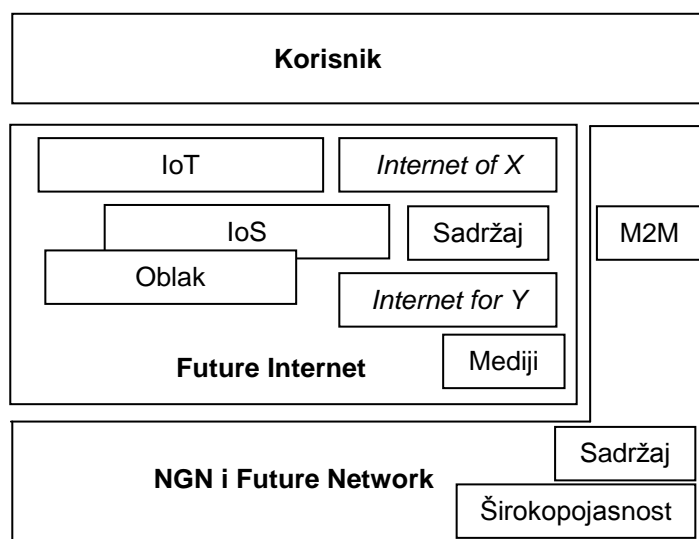
Ovisnost o Internetu je evidentna, ne samo njegov društveni i gospodarski utjecaj, već i upliv na svakodnevni život. Kao što se navodi u [9], „Kako raste društveni utjecaj Interneta, pravni okvir za reguliranje Interneta postaje sve potrebniji. U kontekstu Interneta, a gdje god je primjenjivo, treba koristiti postojeću praksu, regulativu i zakonska rješenja. To implicira da treba uspostaviti arbitracijske procese koji su brzi, s niskim troškovima i učinkoviti. Potrebno je upravljanje Internetom (op.a.: „*governance*“, a ne „*management*“!) u kojem mogu sudjelovati i njegovi korisnici.“

### 6.3. Regulatorna perspektiva

Tehnološko ishodište današnjih telekomunikacijskih mreža je u javnoj telefonskoj mreži s komutacijom kanala, a Interneta u akademskoj računalnoj mreži s komutacijom paketa u SAD. Njihova regulatorna povijest isto je tako različita: državno regulirana liberalizacija telekomunikacija a Internet bez regulacije u povjerljivom okružju. Digitalne tehnologije koje su potaknule i omogućile konvergencijske procese praktički su izbrisale razliku između mreža: mrežni protokol IP primjenjuje se u svim mrežama; sve mreže pristupaju Internetu. Tako su osnovna obilježja NGN-a paketska komutacija i IP-zasnovane usluge, s odvojenim uslužnim i transportnim funkcijama.

Transformacija mrežne arhitekture i modela pružanja usluga s implikacijama na tržište elektroničkih komunikacija, predstavljaju izazove za regulatorna tijela [10].

Novi zahtjevi koji se odnose na svjesnost o uslugama i sadržaju, računalne mogućnosti, sveprisutni širokopojasni pristup i pokretljivost, masovno povezivanje uređaja i objekata reflektiraju se na sigurnost, privatnost i zaštitu podataka. U uporabi su IoT, računarstvo u oblaku kao omogućitelj Interneta usluga (engl. *Internet of Services*, IoS), M2M i nove paradigme rukovanja sadržajem i medijima na Internetu (Slika 4.1.).



**Slika 4.1.** Istraživački prostor

Iako u istraživačkoj zajednici nema jedinstvenog stava kako se približiti budućem Internetu (sve iznova ili evolucija postojećeg), za očekivati je da će prevladati realističniji pristup evolucijskom razvoju Interneta, prihvatljiv za ICT-sektor i regulatore.

#### 6.3.1. Internet stvari i komunikacija strojeva

Ne postoji jednoznačna definicija i objašnjenje Interneta stvari. Europski projekt CASAGRAS pojašnjava paradigmu IoT ovako: „Globalna mrežna infrastruktura koja povezuje fizičke i virtualne objekta iskorištavajući dohvat podataka i komunikacijske mogućnosti. Ta infrastruktura uključuje postojeći i nastajući Internet i razvoj mreža. Omogućit će specifičnu identifikaciju objekata, senzore i povezivanje kao osnovu za razvoj neovisnih kooperativnih

usluga i aplikacija. Sve će biti obilježeno visokim stupnjem samostalnog prikupljanja podataka, prijenosa događaja, mrežnog povezivanja i međudjelovanja.“ [11]

Sadašnji Internet je pretežno mreža povezanih računala, dok Internet stvari predočuje mrežu međusobno povezanih objekata u kojoj pojam „stvari“ pokriva široki spektar aktivnih uređaja kao su senzori, mjerači, aktuatori ili druge naprave, kao i „čiste“ stvari, primjerice različite proizvode i dobra, njihove komade, dijelove ili pakovanja [12, 13]. IoT podržava komunikaciju stvari s osobama, osoba sa stvarima i stvari međusobno. Primjene nisu ničime ograničene. Sustavnim istraživanjima ustanovljeno je dvadesetak područja masovne primjene IoT-a [14]. Riječ je o veoma različitim područjima u kojima se ostvaruju usluge za industriju (energija, transport, proizvodnja, hrana i drugo), kao i one izravno povezane s ljudima (medicina, zdravstvena zaštita, samostalno življenje i drugo).

Koncept komunikacije strojeva (M2M) odnosi se na fizičko povezivanje i izmjenu podataka između „strojeva“ putem telekomunikacijske mreže. Pojam „stroja“ odgovara pojmu „stvari“. [15]. M2M se može promatrati kao podskup od IoT, sa specifičnim rješenjima platformi i dodatnim rješenjima primjerenim pokretnoj mreži [16].

Od posebne su važnosti za IoT-usluge njihov kontinuitet i raspoloživost. Dodatno, za kritične sustave i infrastrukturu kao što je energija, treba postići zahtijevanu pouzdanost. Specifična rješenja istražuju se u okviru Interneta energije (engl. *Internet of Energy*, IoE) [17].

Treba naglasiti potencijalne probleme vezane uz privatnost: posredno je moguće povezati stvar s osobom, npr. stvar pripada osobi ili se nalaze u istom prostoru. Mogućnost lociranja stvari predstavlja prijetnju privatnosti i kad osoba nije izravno povezana s nekom stvari. Europski akcijski plan za IoT, uz opća načela upravljanja i odgovornosti, ističe važnost rješenja za sigurnost, privatnost i zaštitu osobnih podataka [18-21].

Osnovni zahtjevi na IoT vezani uz informacijsku sigurnost su sljedeći:

- Tajnost: informacija nije dostupna ili izložena neovlaštenim osobama, entitetima ili procesima;
- Cjelovitost: točnost i potpunost informacije;
- Raspoloživost: informacija je dostupna na zahtjev i omogućeno je njeno korištenje od strane ovlaštenih osoba, entiteta ili procesa;
- Vjerodostojnost: osoba, entitet ili proces je zaista onaj kojim se predstavlja;
- Odgovornost: obveza izvještavanja o aktivnostima i preuzimanja odgovornosti za njih;
- Neporicanje: sposobnost dokazivanja događaja ili aktivnosti i osoba, entiteta ili procesa koji su ih pokrenuli ili u njima sudjelovali;
- Pouzdanost: konzistentno ponašanje i rezultati.

Definicija sadržana u [22] ovdje je proširena na IoT i M2M: „entitet“ odgovara „stvari/stroju“, „informacijom“ se smatra bilo koja vrsta podataka kojeg izmjenjuju stvari/strojevi, ili se izmjenjuje sa stvarima/strojevima, ili procesima koji njima rukuju.

Očevidno je da dio rješenja vezanih uz privatnost i zaštitu podataka zahtijeva sigurnu mrežu, usluge i aplikacije.

### 6.3.2. Internet usluga i računarstvo u oblaku

Internet usluga (IoS) je koncept pružanja i korištenja usluga koji se temelji na uslužno-zasnovanoj arhitekturi, webu (engl. *World Wide Web*, WWW), semantičkim tehnologijama i raspodijeljenom računarstvu na zahtjev (engl. *on-demand distributed computing*). IoS treba omogućiti tako jednostavan pristup uslugama kakav je uobičajen za podatke i informacije.

Računarstvo u oblaku kao raspodijeljeno okružje koje omogućuje obradu na zahtjev tretira se kao omogućitelj Interneta usluga [23].

Američki *National Institute of Standards and Technology* (NIST) definira računarstvo u oblaku ovako „Model koji omogućuje sveprisutni, prikladni i na zahtjev ostvareni mrežni pristup dijeljenoj skupini konfigurabilnih računalnih resursa (mreže, poslužitelji, memorijski prostor, aplikacije i usluge) koji se mogu pružiti i osloboditi u kratkom vremenu, s malim udjelom upravljanja ili međudjelovanja davatelja usluga“ [24].

Računarstvo u oblaku uključuje više modela pružanja usluga:

- Softver kao usluga (engl. *Software as a Service*, SaaS),
- Platforma kao usluga (engl. *Platform as a Service*, PaaS),
- Infrastruktura kao usluga (engl. *Infrastructure as a Service*, IaaS),

i dodatno za telekomunikacijski usredotočene oblake:

- Komunikacija kao usluga (engl. *Communications as a Service*, CaaS) i
- Mreža kao usluga (engl. *Network as a Service*, NaaS).

Ovo su modeli za pristup softveru, platformi i infrastrukturi po potrebi, tj. na zahtjev. Oni nude dobra nefunkcijska obilježja kao što su skalabilnost, raspoloživost, pouzdanost i elastičnost, sukladno zahtjevima usluge, i time utječu na smanjenje troškova.

U mnogim se radovima pokazuje potencijalni utjecaj računarstva u oblaku na produktivnost, gospodarski rast i zapošljavanje, zajedno s upozorenjima na moguće prepreke, od kojih su neke regulatorno važne. To se odnosi posebice na zaštitu podataka, uključujući probleme uz velike količine podataka (engl. *Big Data*) i privatnost [25]. Isto tako, mnoge studije naglašavaju potrebu za intenziviranjem istraživanja inovativnih tehnologija koje će omogućiti takvu ulogu računalnog oblaka [26].

Uska je povezanost komuniciranja i računanja tako da svaki tehnički ili netehnički problem na komunikacijskoj ili računalnoj strani negativno utječe na uslugu, njen kontinuitet i kvalitetu. Iz toga proizlaze zahtjevi za usklađenom i konzistentnom regulativom [27]. Širokopojasni pristup i povezanost, kao i mrežna neutralnost su opće komunikacijske teme, dok sigurnost, privatnost i zaštita podataka utječu i na komunikacije i na računarstvo.

Nakon kratke ranije rasprave sigurnosnih aspekata IoT, ukratko se navode pitanja privatnosti i zaštite podataka u računalnom oblaku. Naime, oblak potencijalno izlaže riziku sve podatke i usluge koje sadrži iz sljedećih razloga: a) arhitektura oblaka (sveprisutni mrežni pristup, dijeljeni računalni resursi), b) način rada (na zahtjev), c) organizacija i vlasništvo oblaka (privatno, javno, hibridno). Posebno je pitanje osobnih podataka, jer je pravom na privatnost jasno određeno pravo osobe da kontrolira vlastite osobne, javne ili profesionalne podatke.

Potreban je novi pristup, tzv. uvažavanje privatnost tijekom oblikovanja usluga (engl. *privacy-by-design*), a nakon toga u cijelom njenom životnom ciklusu. Zaštita podataka zahtijeva ispunjavanje uvjeta tajnosti, cjelovitosti i vjerodostojnosti. Uz to, potrebno je minimalizirati i ograničiti uporabu podataka, odnosno: a) ne koristiti ih, ili ih koristiti u najmanjoj mogućoj mjeri, b) sigurnosno odvojiti različite funkcije. Da bi se ostvarilo pravo na kontrolu rukovanja osobnim podacima, treba uspostaviti sučelja koja će to omogućiti. Dodatno, podaci trebaju biti dostupni za posebne zakonom određene potrebe.

#### **6.4. Regulatorni prostor**

Iskustva iz regulacije elektroničkih komunikacija i Interneta ukazuju na širok raspon pristupa i regulatornih instrumenata koji su se primjenjivali i koji se primjenjuju. Riječ je o sljedećim konceptima:

- Bez regulacije: bez eksplicitne kontrole, što je primjenjivo u situacijama u kojima konkurentno tržište postiže željene ciljeve samo po sebi (npr. mogućnost odabira davatelja usluge, prihvatljive cijene), a što je tipično za ranu primjenu novih tehnologija.
- Samoregulacija (engl. *self-regulation*): industrija (komunikacijska, računalna, medijska, ICT u cijelosti) postavlja, uvodi i administrira regulatorne ciljeve bez formalnog nadzora vlade ili regulatornog tijela.
- Koregulacija (engl. *co-regulation*): industrija i javna tijela zajedno određuju regulatorna rješenja, a vlada ili regulatorna tijela određuju pravni okvir za njihovu primjenu.
- Statutarna regulacija (engl. *statutory regulation*): regulatorna tijela propisuju regulatorne ciljeve i pravila, kao i zahtjeve na davatelje usluga. Ovaj način regulacije primjenjuje se u okolnostima u kojima postoje davatelji usluga sa značajnom tržišnom snagom, ili različiti interesi u industrijama onemogućuju postizanje zajedničkih rješenja.

Nekoliko primjera pokazat će regulatorne alternative.

Internet je pokrenut u SAD kao međusveučilišna paketska mreža koja povezuje računala kao krajnje sustave. To je bilo razdoblje bez ikakve regulacije. Širenjem Interneta, najprije kao akademske mreže, javlja se potreba za sustavnim istraživanjem njegove arhitekture, protokola i načina rada, kao i uspostavljanja normizacijskih procesa koji obuhvaćaju specifikaciju pojedinih rješenja te njihovu evaluaciju, prihvaćanje i reviziju u internetskoj istraživačkoj zajednici. Tu ulogu preuzima tijelo *Internet Engineering Task Force* (IETF) osnovano 1986., kao otvoreno standardizacijsko tijelo bez formalnog članstva. Misija IETF-a opisana je ovako

„Stvaranje visokokvalitetnih i relevantnih tehničkih i inženjerskih dokumenata koji utječu na način kako se oblikuje, koristi i upravlja Internet tako da bi radio sve bolje. Ti dokumenti uključuju standarde protokola, primjere najbolje prakse i različite vrste informacija“. [28] To je razdoblje u kojem se primjenjuju načela samoregulacije. Isto vrijedi za *World Wide Web Consortium* (W3C), glavno standardizacijsko tijelo za WWW osnovano 1994.

*Internet Corporation for Assigned Names and Numbers* (ICANN) pokrenut 1998, koordinira aktivnosti internetskog globalnog sustava domenskih naziva. Unutar ICANN-a, *Governmental Advisory Committee* (GAC) „ima savjetodavnu ulogu u javnoj politici, posebice kad se javlja međudjelovanje aktivnosti u ICANN-u s drugim politikama, nacionalnim zakonodavstvom ili međunarodnim sporazumima“. To bi bio način koregulacije u kojem Europska unija zagovara višedionički (engl. *multi-stakeholder*) pristup upravljanju Internetom, umjesto sadašnjeg operativnog sporazuma ICANN-a s američkom vladom.

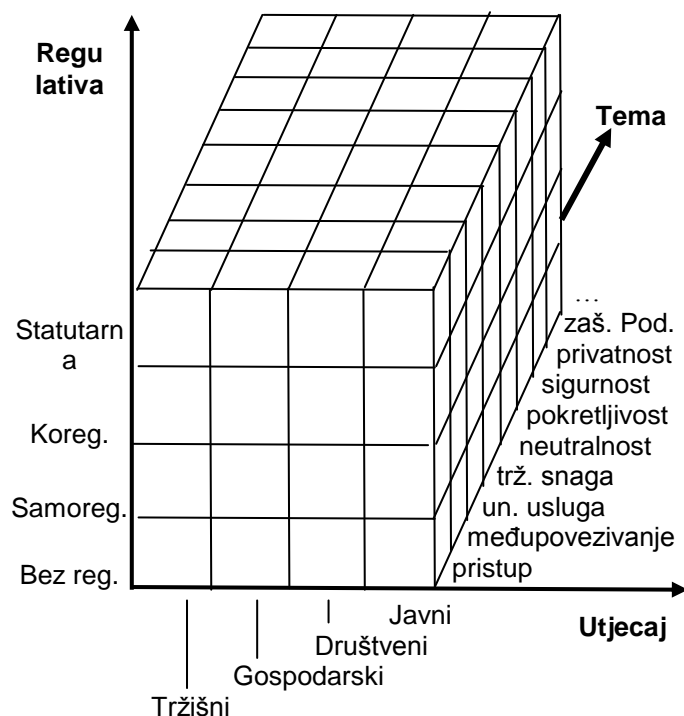
Telekomunikacije su prošle potpuno drukčiji put, od državnog monopola do konkurentnog tržišta elektroničkih komunikacija koji je vođen statutarnom regulacijom. Postojeća situacija u EU definirana je zajedničkim regulatornim okvirom za elektroničke komunikacije [29]. Sukladno Okvirnoj direktivi (engl. *Framework Directive*), nacionalna regulatorne tijela trebaju „pridonijeti razvitku unutarnjeg tržišta“, „promovirati interese građana“ i „promovirati konkurenciju u pružanju elektroničkih komunikacijskih mreža, elektroničkih komunikacijskih usluga i pridruženih sredstava i usluga, među kojima: a) osigurati da korisnici, posebno korisnici s posebnim potrebama, dobiju najbolji mogući odabir, cijenu i kvalitetu usluga; b) osigurati da nema narušavanja ili ograničenja tržišnog natjecanja u sektoru elektroničkih komunikacija, c) poticati učinkovita ulaganja u infrastrukturu i osigurati učinkovito upravljanje radiofrekvencijskog spektra i numeracije.“ [30, 31]

Da sada su se primjenjivali različiti pristupi regulaciji pojedinih pitanja, a regulatorni ciljevi mijenjali sukladno tehnološkim i tržišnim promjenama. Takav će pristup biti potreban i ubuduće, ali za očekivati je sve brže promjene. Razvoj ICT-a, uključujući mreže, usluge, aplikacije i sadržaje je izvanredan, kao i rezultati istraživanja, razvoja i inovacija u ovom području. To se treba odraziti na upravljanje i reguliranje elektroničkih komunikacija, uključujući Internet – prilagodba okružju koje se mijenja je neophodna, kao i priprema rješenja za to.

Internet i komunikacijske mreže u cijelosti su područje intenzivnog istraživanja usmjerenog budućnosti, u mnogim slučajevima s obilježjima graničnih istraživanja (engl. *frontier research*). Elektroničke komunikacije su posebno ovisne o istraživanju, razvoju i inovacijama. Isto tako one potiču razvoj i inovacije u drugim područjima, otvaraju nove usluge i nova tržišta za sadašnje i nove sudionike. Stoga sam regulatorni prostor treba obuhvatiti tehnološki razvoj i tehnološku politiku.

Različite vrste probleme traže različite regulatorne instrumente, odnosno različita rješenja za različite okolnosti. Prepoznata je potreba za pametnom regulacijom (engl. *smart regulation*) koja je učinkovita i usmjerena na probleme, a kreće se od rješenja bez regulacije ili deregulaciju, preko samoregulacije i koregulacije, do statutarne regulacije, ovisno o prirodi

problema [32, 33, 34]. Takav regulatorni prostor i njegove tri dimenzije predočeni su na slici 4.2.



**Slika 4.2.** Regulatorni prostor

To je izvorni model regulatornog prostora koji se ovdje predlaže u cilju konceptualnog i operativnog sagledavanja regulatornih aktivnosti primjerenih dinamici razvoja tržišta.

Uz regulatornu dimenziju (bez regulacije, samoregulacija, koregulacija, statutarna regulacija) uvode se dvije dodatne dimenzije:

- Utjecaj:
  - Tržišni
  - Gospodarski
  - Društveni
  - Javni
- Tema:
  - Pristup
  - Međupovezivanje
  - Univerzalna usluga
  - Tržišna snaga
  - Mrežna neutralnost
  - Sigurnost
  - Pokretljivost

- Privatnost
- Zaštita podataka
- Itd.

Promjene se očekuju i u načinu kao se provodi regulacija: od vertikalnih rješenja za specifičnu mrežu ili uslugu prema rješenjima za više, u nekim slučajevima sve mreže i usluge. Takva su rješenja primjerena za mnoge sustave i usluge koji kombiniraju različite paradigme. Uzmino za primjer prikupljanje podataka sensorima primjenom IoT i njihovu pohranu i obradu u računalnom oblaku [35].

### **6.5. Zaključno razmatranje**

Sadašnje stanje elektroničkih komunikacija i primjena europskog regulatornog okvira obuhvaćeni su u [36]. Manja tržišta, kao što je hrvatsko tržište elektroničkih komunikacija, neće se razvijati sama po sebi, samo zbog globalnog razvoja. Tri su opće pretpostavke za razvoj nacionalnog tržišta: višedionički pristup u Hrvatskoj, regulator sa znanjem potrebnim za složeni i dinamični regulatorni prostor te uključenost u međunarodne aktivnosti, istraživačke i regulatorne.

Potrebno je naglasiti važnost višedioničkog pristupa. Već je rečeno da se u elektroničkim komunikacijama brišu granice sadašnje-novo, novo-buduće, a razvojni zahtjevi u regulatornoj domeni preklapaju se s onima vezanima uz razvoj digitalnog društva i gospodarstva [37, 38]. Riječ je o novom i stabilnom širokopojasnom regulatornom okružju, novoj javnoj digitalnoj uslužnoj infrastrukturi, strategiji kibernetičke sigurnosti, bržem uvođenju usluga u oblaku, pitanjima upravljanja Internetom, regulacije sadržaja i podataka, dominacije na tržištu. To bi trebala obuhvatiti Digitalna agenda za Hrvatsku. Primjena trodimenzionalnog modela regulatornog prostora omogućit će uravnoteženi pristup konkurenciji i ulaganju koji generira rast.

Regulatorni izazovi koji proizlaze iz IoT, M2M, IoS i računarstva u oblaku, a koji su koraci u ostvarivanju „*Future Network*“ i „*Future Internet*“ pokreću potrebu za stvaranjem skupa usklađenih i konzistentnih regulatornih instrumenata za pametnu regulaciju. Takav pristup globalnih i nacionalnih regulatora zasnovan na višedioničkom modelu pridonijet će ciklusu digitalne ekonomije, održati Internet otvorenim i inovativnim, a mreže atraktivnima za ulaganja.

### **6.6. Literatura**

[1] “Future Networks: Objectives and design goals”, Recommendation ITU-T Y-3001, ITU-T Telecommunication Standardization Sector of International Telecommunication Union, Geneva, 2011.

[2] J. Pan, S. Paul, R. Jain, “A Survey of the Research on Future Internet Architectures”, IEEE Communications Magazine, Vol. 49, No. 7, pp. 26-36, 2011.

[3] S. Paul, R. Jain, „Architectures for the future networks and the next generation Internet: A survey“, Computer Communications 34 (2011), pp. 2–42, 2011.



- [4] A. Galis, A. Gavras (Eds.), “Future Internet, Future Internet Assembly 2013: Validated Results and New Horizons”, Lecture Notes in Computer Science, Vol. 7858, Springer, 2013.
- [5] “The Future of the Internet, A Compendium of European Projects Supported by the 7<sup>th</sup> Framework Programme for RTD”, European Commission, Information Society and Media, 2008.
- [6] D. Matsubara, T. Egawa, N. Nishinaga, M-K. Shin, V.P. Kafle, A. Galis, “Open the Way to Future Networks – A Viewpoint Framework form ITU-T”, “Future Internet, Future Internet Assembly 2013: Validated Results and New Horizons”, Lecture Notes in Computer Science, Vol. 7858, pp. 27-38, Springer, 2013.
- [7] “Future Internet and NGN, Design requirements and principles for a Future Media and 3D Internet”, European Commission, Information Society and Media, 2009.
- [8] “Future Internet Design Principles”, European Commission, Information Society and Media, 2012.
- [9] „Towards a Future Internet, Interrelation between Technological, Social and Economic Trends“, Final Report for DG Information Society and Media, European Commission DG INFSO Project SMART 2008/0049, 2010.
- [10] I. Lovrek, D. Lucic, G. Gacina, „Next Generation Network and Regulatory Challenges”, Proceedings SoftCOM 2011 19<sup>th</sup> International Conference on Software, Telecommunications and Computer Networks, Workshop on Regulatory Challenges, Split-Hvar-Dubrovnik, Croatia, 2011.
- [11] “RFID and the Inclusive Model of the Internet of Things, Final Report”, CASAGRAS an EU Framework 7 Project “Coordination And Support Action for Global RFID-related Activities and Standardisation”, 2009.
- [12] L. Atzori, A. Iera, G. Morabito, “The Internet of Things: A Survey”, Computer Networks, 54(2010), pp. 2787-2805, 2010.
- [13] J. Gubbi, R. Buyya, S. Marusic, M. Palaniswami, “Internet of Things (IoT): A vision, architectural elements and future directions”, Future Generation Computer Systems, 29(2013), pp. 1645-1660, 2013.
- [14] H. Sundmaeker, P. Guillemin, P. Friess, S. Woelfflé (eds.) „Vision and Challenges for Realising the Internet of Things“, European Commission, Information Society and Media, 2010.
- [15] „Machine-to-Machine communications (M2M); Definitions“, ETSI TR 102 725 V1.1.1 (2013-06), 2013.
- [16] D. Katusic, M. Weber, I. Bojic, I. G. Jezic, M. Kusek, „Market, standardization, and regulation development in Machine-to-Machine communications”, Proceedings SoftCOM 2012 20<sup>th</sup> International Conference on Software, Telecommunications and Computer

Networks, The 2nd Workshop on Regulatory Challenges in the Electronic Communications Market, Split, Croatia, 2012.

[17] N. Bui, A.P. Castellani, P. Casari, M. Zorzi, “The Internet of Energy A Web-enabled Smart Grid System”, IEEE Network, Vol. 26, No.4, pp. 39-45, 2012.

[18] “Internet of Things – An Action Plan for Europe”, COM(2009) 278 final, Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, 18.6.2009.

[19] R. H. Weber, “Internet of Things – New Security and Privacy Challenges”, Computer Law and Security Review, 26(2010), pp. 23-30, 2010.

[20] R. H. Weber, “Accountability in the Internet of Things”, Computer Law and Security Review, 27(2011), pp. 133-138, 2011.

[21] N. Gumzej, “Protection of Data Relating to EU Consumers in the IoT Age”, Proceedings SoftCOM 2012 20th International Conference on Software, Telecommunications and Computer Networks, The 2nd Workshop on Regulatory Challenges in the Electronic Communications Market Split, Croatia, 2012.

[22] „Information technology — Security techniques — Information security management systems — Overview and vocabulary“, International Standard ISO/IEC 27000, 2014.

[23] R. M. Vozmediano, R. S. Montero, I. M. Lorente, “Key Challenges in Cloud Computing, Enabling the Future Internet of Services”, IEEE Internet Computing, Vo. 17, No. 4, 18-25, 2013.

[24] P. Mell, T. Grance, „The NIST Definition of Cloud Computing“, Special Publication 800-145, NIST National Institute of Standards and Technology, Gaithersburg, MD, USA, September 2011.

[25] “Unleashing the Potential of the Cloud Computing in Europe”, COM(2012) 529 final, Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, 27.9.2012.

[26] L. Schubert, K. Jeffery, B. Neidecker-Lutz (eds.), “A Roadmap for Advanced Cloud Technologies under H2020, Recommendation by the Cloud Expert Group”, Commission of the European Union, Directorate-General for Communication Networks, Content and Technology, Software and Services, Cloud Unit, 2012.

[27] I. Lovrek, T. Lovric. D. Lucic, “Regulatory Aspects of Cloud Computing”, Proceedings SoftCOM 2012 20th International Conference on Software, Telecommunications and Computer Networks, The 2nd Workshop on Regulatory Challenges in the Electronic Communications Market Split, Croatia, 2012.

[28] „A Mission Statement for the IETF“, Request for Comments: 3935, Internet Engineering Task Force, October, 2004.

[29] „Regulatory framework for electronic communications in the European Union“, Commission of the European Union, Directorate-General for Communication Networks, Content and Technology, 2010.

[30] „Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive)“, Official Journal of the European Communities, L 108/33, 24.4.2002.

[31] „Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services“, Official Journal of the European Communities, L 337/37, 9 18.12.2009.

[32] “EU Regulatory Fitness”, COM(2012) 746 final, Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, 12.12.2012.

[33] “Strengthening the foundations of Smart Regulation – improving evaluation”, COM(2013) 686 final, Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, 2.10.2013.

[34] “Trends in Telecommunications Reform 2012: Smart Regulation for a Broadband World”, International Telecommunications Union, 2012.

[35] I. Podnar Zarko, K. Pripuzic, M Soprano, M. Hauswirth, “IoT Data Management Methods and Optimisation Algorithms for Mobile Publish/Subscribe Services in Cloud Environment”, Proceedings EuCNC’2014 European Conference on Networks and Communications Conference Proceedings, Bologna, Italy, 2014.

[36] “Implementation of the EU Regulatory Framework for electronic communications – 2014”, Commission Staff Working Document, SWD(2014)249 final European Commission, 14.7.2014.

[37] „A Digital Agenda for Europe“, Communications from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions, COM(2010) 245, Brussels, Belgium, 19.5.2010.

[38] „The Digital Agenda for Europe – Driving European Growth digitally“, Communications from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions, COM(2010) 784, Brussels, Belgium, 18.12.2012.

## **7. Istraživanje o troškovnim metodologijama u informacijskim sustavima operatora u RH**

### **7.1. Uvod**

Zahvaljujući nekonzistentnosti u regulaciji troškova završavanja poziva (engl. *Call termination rate*), u većini država članica EU postoje značajne razlike u odabranim troškovnim instrumentima te, također, različite prakse u implementaciji istih. Značajno odstupanje u regulatornom tretmanu cijena završavanja poziva fiksne i mobilne mreže uzrokuje osnovne konkurentske deformacije. Tržišta završavanja poziva predstavljaju situaciju dvosmjernog pristupa gdje se za oba operatora, koja omogućavaju poziv, pretpostavlja da imaju koristi od aranžmana. Međutim, kako ti operatori međusobno konkuriraju među korisnicima, cijene poziva mogu imati važne strateške i konkurentske implikacije. Određivanje cijena poziva iznad učinkovitih troškova uzrokuje značajne transfere između tržišta fiksne i mobilne mreže te korisnika. Osim toga, na tržištima na kojima operatori imaju asimetrične tržišne udjele može doći do značajnih plaćanja operatora s manjim tržišnim udjelom operatorima s manjim tržišnim udjelom. Generalno gledajući, cijene završavanja poziva za krajnje korisnike u mobilnoj i fiksnoj mreži na području EU su visoke te sporo padajuće. Visoke cijene završavanja poziva imaju tendenciju dovođenja do visokih maloprodajnih cijena odlaznih poziva i, sukladno tome, niže stope iskoristivosti te se tako smanjuje korisnička dobrobit. Svjesni spomenute situacije, Europska Komisija donijela je Preporuku o regulatornom tretmanu cijena poziva u fiksnoj i mobilnoj mreži na području EU, 7. svibnja 2009. Preporuka se sastoji od 14 prijedloga koji su zapravo načela za izračun veleprodajnih cijena završetka poziva u fiksnoj i mobilnoj mreži. Predlaže se evaluacija učinkovitih troškova zasnovana na tekućem trošku (engl. *Current Cost Accounting*) i pristup „odozdo prema gore“ pri korištenju dugoročnih inkrementalnih troškova (engl. *Long-run incremental costs*) kao relevantne troškovne metodologije. U ovom radu bit će prikazan teoretski okvir troškovne metodologije za raspodjelu troškova u telekomunikacijskoj industriji koju preporučuje Europska Unija, te troškovna metodologija koja se trenutno koristi u telekomunikacijskoj industriji.

Glavna karakteristika telekomunikacijskog sektora su stalne tehnološke promjene koje sa sobom nose strukturne promjene u troškovima. Većina troškova u telekomunikacijskim kompanijama su indirektni troškovi, čak do 80% ukupnih troškova, koje nije lako raspodjeliti na troškovne objekte te se zato javlja potreba za transparentnim troškovnim upravljanjem.

Cilj je učinkovitog upravljanja troškovima unaprijediti poslovne procese smanjivanjem broja onih aktivnosti koje se odvijaju unutar poduzeća, a zapravo nemaju nikakvu vrijednost za korisnika usluga kao i obavljanje aktivnosti poduzeća u što kraćem vremenu. Na menadžmentu je da prije implementacije bilo kojeg sustava upravljanja troškovima, odredi ciljeve koje poduzeće želi postići te da upozna zaposlenike s postavljenim ciljevima. Mnogi su faktori zbog kojih je bitno pronaći adekvatnu metodu raspoređivanja troškova koja će reflektirati vezu između nastalih troškova i ključa za raspored istih na nositelje. To su proces

globalizacije, zatim regulatorni utjecaj od strane državne agencije, brza supstitucija starih usluga novim uslugama i slično.

Tradicionalne metode ne uspijevaju dati kvalitetne i transparentne informacije o troškovima usluga odnosno te metode karakterizira nepostojanje jasne uzročno-posljedične veze između nastalih troškova i ključa za raspored troškova na nositelje te se javlja potreba za novim metodologijama i metodama. Tako danas postoje dvije troškovne metodologije u telekomunikacijskoj industriji, metodologija potpuno raspodjeljenih troškova (engl. *Fully Allocated Costs*, FAC) i metodologija dugoročno inkrementalnih troškova (engl. *Long Run Incremental Costs*, LRIC), koje će biti predmetom istraživanja. Važnost FAC metodologije je u metodi obračuna troškova prema aktivnostima (engl. *Activity Based Costing*, ABC) koja se koristi za računovodstveno praćenje dok se važnost LRIC metodologije očituje u korištenju za regulatorne svrhe.

Cilj ovog rada je istražiti računovodstveno informacijski sustav u telekomunikacijskoj industriji, te odabir najbolje s ciljem učinkovitog upravljanja troškovima u spomenutoj industriji. Kako su strukturne promjene u troškovima jedna od glavnih karakteristika telekomunikacijskog sektora, gledano iz ekonomske perspektive, bitno je naći odgovarajuće instrumente za raspoređivanje istih s ciljem unaprjeđenja poslovnih procesa.

## **7.2. Rezultati empirijskog istraživanja**

Cilj anketnog upitnika, koji je razvijen za potrebe izrade specijalističkog rada „Odabir instrumenta za upravljanje troškovima u telekomunikacijskoj industriji“<sup>1</sup>, je istražiti postojeće računovodstvene informacijske sustave (RIS) telekomunikacijskih operatora u Republici Hrvatskoj, donijeti opće zaključke o kvaliteti te mogućem poboljšanju i nadogradnji istih.

Javno dostupnu telefonsku uslugu u nepokretnoj elektroničkoj komunikacijskoj mreži trenutno pruža 49 registriranih operatora, dok javno dostupnu telefonsku uslugu u pokretnoj elektroničkoj komunikacijskoj mreži trenutno pružaju tri operatora u Republici Hrvatskoj. Anketni upitnik poslan je svim registriranim operatorima u pokretnoj i nepokretnoj mreži, međutim samo se njih šestero odazvalo na istraživanje i ispunilo anketni upitnik.

Tablica 5.1. prikazuje opće informacije telekomunikacijskih operatora koji su sudjelovali u anketnom istraživanju. Kako im je tijekom istraživanja zajamčena privatnost podataka, umjesto njihovih imena dane su im numeričke oznake od 1 do 6 koliko ih je i sudjelovalo u istraživanju.

---

<sup>1</sup> Ivić, M., (2014): Odabir instrumenta za upravljanje troškovima u telekomunikacijskoj industriji, specijalistički završni rad, Fakultet elektrotehnike i računarstva Sveučilišta u Zagrebu, obranjen u svibnju 2014. godine.

Tablica 5.1. Opće informacije o telekomunikacijskim operatorima

NAZIV	1	2	3	4	5	6
<b>VELIČINA (ZOR)</b> mali (0-50) srednji (51-250) veliki (251-500+)						
	veliki	veliki	veliki	srednji	srednji	srednji
<b>PRAVNI OBLIK</b>	dioničko društvo	društvo s ograničenom odgovornošću	dioničko društvo	dioničko društvo	društvo s ograničenom	dioničko društvo
<b>STRUKTURA VLASNIŠTVA</b>	51% inozemni telekomunikacijski operator, 3.5% privatni i institucionalni investitori, 7%	100% inozemni telekomunikacijski operator	privatno vlasništvo	privatno vlasništvo	inozemni investicijski fondovi	100% domaći telekomunikacijski operator
<b>STRUKTURA VLASNIŠTVA</b>	umirovljenički fond 3.5%, privatni i	A1 Telekom Austria	privatno vlasništvo	privatno, domaće	fondovi IRIS, KBC	100% Hrvatski Telekom
<b>BROJ KORISNIKA</b>	4,5 milijuna korisnika	2,1 milijuna korisnika	220 000	10 000	2 000	100 000
<b>BROJ ODJELA</b>	33	4 sektora	25	28 (9 sektora)	9	28
<b>POSTOJEĆI ODJELI</b>						
računovodstvo	+	+	+	+	+	+
analiza	+	+				+
financije	+	+	+	+		+
kontroling	+	+	+		+	+
ljudski potencijali	+	+	+			+
opći poslovi	+	+	+		+ (pravni poslovi i regulativa)	+
zaštita na radu	+	+				+
razvoj	+	+		+		+
priprema	+	+				
kvaliteta	+	+				
proizvodnja	+	+			+ (tehnika)	
skladištenje	+	+			+	
održavanje	+	+	+		+ (korisnička služba)	+
istraživanje tržišta	+	+				+
oglašavanje	+	+			+	+
nabava	+	+	+			+
logistika	+	+	+			+
prodaja	+	+	+	+ (2: Zg+regija)	+	+
ostalo	sektor za transformaciju, e-poslovanje, informacijski sustavi		tehnika, operativni poslovi	sektor za odnose s korisnicima, 3 tehnička sektora	administracija, naplata	tehnika

Izvor: Empirijsko istraživanje

Tablica 5.2. prikazuje sve vrste usluga koje pružaju operatori koji su sudjelovali u anketnom istraživanju.

**Tablica 5.2.** Vrste usluga koje pružaju anketirani operatori

PRUŽENE USLUGE	1	2	3	4	5	6
Javno dostupna telefonska usluga u nepokretnoj elektroničkoj komunikacijskoj mreži	+	+	+	+	+	+
Javno dostupna telefonska usluga u pokretnoj elektroničkoj komunikacijskoj mreži	+	+				
Davanje u najam elektroničke komunikacijske mreže i/ili	+	+	+	+	+	
Usluga prijenosa slike, govora i zvuka putem elektroničkih komunikacijskih mreža (što isključuje usluge radiodifuzije)	+	+	+	+	+	+
Usluge u privatnoj pokretnoj mreži (PMR)	+					
tarifom i besplatnog poziva	+	+	+	+	+	+
Usluge davanja pristupa interneta	+	+	+	+	+	+
Usluge prijenosa govora putem interneta	+	+	+	+	+	
multipleksom u radiodifuziji	+					
Usluge prijenosa, odašiljanja i/ili prijama slike, govora, zvuka te drugih podataka	+					
Usluge u satelitskoj službi	+	+	+			
Davanje pristupa i zajedničkog korištenja elektroničke komunikacijske infrastrukture i povezane	+			+	+	
Davanje obavijesti (informacija) o brojevima svih pretplatnika javno dostupnih telefonskih usluga u Republici	+	+				
Izdavanje sveobuhvatnog javnog imenika svih pretplatnika u Republici Hrvatskoj	+					
Usluge mobilnog virtualnog mrežnog	+					
Ostale usluge	ICT usluge, prodaja el. Energije					

*Izvor: Empirijsko istraživanje*

Slika 5.1. prikazuje standarde financijskog izvještavanja koje koriste operatori pri sastavljanju financijskih izvještaja. Jedan operator koristi Hrvatske standarde financijskog izvještavanja (HSFI), četiri operatora koriste Međunarodne standarde financijskog izvještavanja (MSFI)<sup>2</sup>, te

<sup>2</sup> Narodne novine, broj 136, Zagreb, 12. Studenog 2009., s Interneta, <http://www.osfi.hr/Uploads/1/2/21/46/100/Odluka.pdf>, 02.03.2014.

jedan koristi i jedne i druge. HSFI nastali su sukladno Zakonu o računovodstvu, a donosi ih Odbor za standarde financijskog izvještavanja. Oni se temelje na domaćoj računovodstvenoj teoriji i praksi, odrednicama MSFI-a kao i na IV. i VII. Direktivi Europske unije. HSFI-ovima regulira se tematika u vezi s financijskim izvještajima, u prvom redu, namijenjenih vanjskim korisnicima. Oni sadrže zahtjeve priznavanja, mjerenja, procjenjivanja, prezentiranja i objavljivanja transakcija i događaja važnih za financijske izvještaje opće namjene. HSFI su namijenjeni za primjenu u financijskim izvještajima opće namjene poduzetnika koji ostvaruju dobit ili gubitak. Pojam financijski izvještaj obuhvaća cjelovit skup financijskih izvještaja sastavljenih za razdoblje tijekom godine ili za poslovnu godinu. Oni reguliraju sastavljanje, prezentiranje i objavljivanje financijskih izvještaja za poduzetnike koji nisu obveznici primjene MSFI, a u skladu sa Zakonom o računovodstvu. Posebno su prilagođene potrebama srednjih i malih poduzetnika koji su prevladavajući u hrvatskom gospodarstvu. S tim u svezi HSFI su jednostavni, malog su opsega te teoretski i stručno zadovoljavaju kriterije suvremenog financijskog računovodstva. HSFI zadovoljavaju uvjete koje Europska unija postavlja glede sastavljanja, prezentiranja i objavljivanja financijskih izvještaja. Kriteriji mjerenja i priznavanja u suglasju su s MSFI, kao i sa IV. i VII. Direktivom EU. Poduzetnici čiji su financijski izvještaji u skladu s HSFI trebaju objaviti u bilješkama izjavu o njihovoj primjeni i sukladnosti. HSFI karakterizira dinamičnost, odnosno prilagođavanje zahtjevima struke, izmijenjenim, dopunjenim i prilagođenim MSFI i IV. i VII. Direktivi EU.<sup>3</sup> Obveznici primjene HSFI-a su mali i srednji poduzetnici, odnosno poduzeća koje zadovoljavaju sve sljedeće kriterije:<sup>4</sup>

- poduzeća čije dionice ne kotiraju na burzi;
- nisu financijske institucije;
- ne sastavljaju konsolidirana financijska izvješća;
- ne zadovoljavaju 2 ili 3 od 3 kriterija vezanih za visinu aktive (više od 108 milijuna kuna), prihoda (više od 216 milijuna kuna) i broj zaposlenika (više od 250 zaposlenika) potrebnih za klasifikaciju u skupinu velikih poduzetnika sukladno Zakonu o računovodstvu.

Međunarodni standardi financijskog izvještavanja jedinstveni su set kvalitetnih globalnih računovodstvenih standarda koji predstavljaju podlogu za sastavljanje transparentnih i usporedivih računovodstvenih informacija prezentiranih u obliku temeljnih financijskih izvještaja.<sup>5</sup>

---

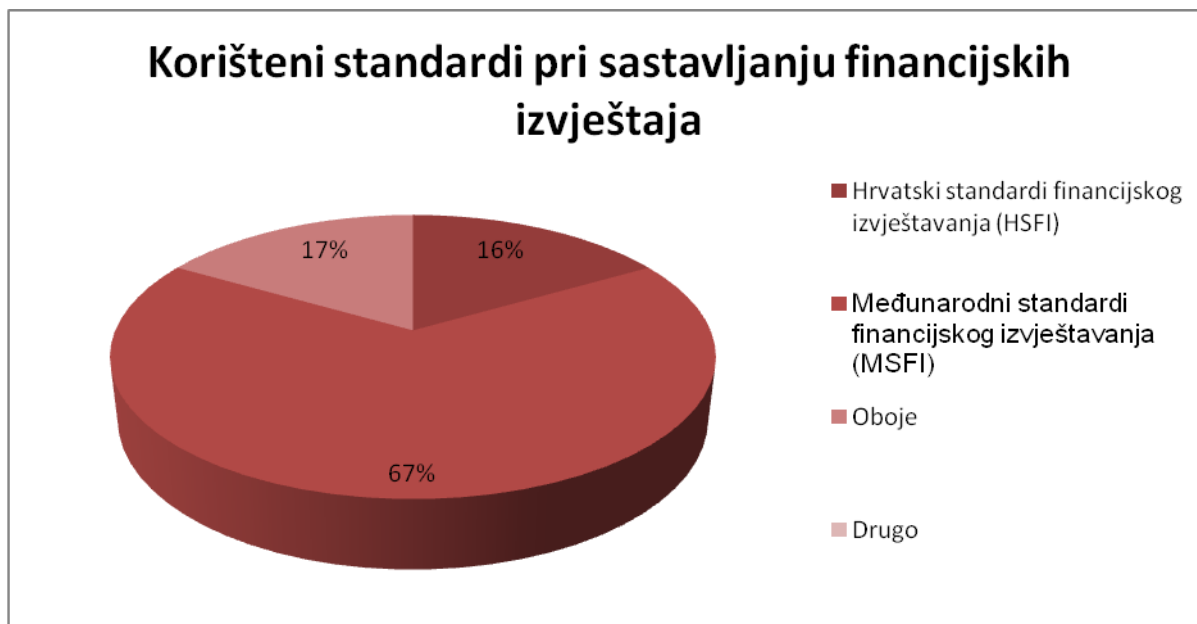
<sup>3</sup> Smiljan, I.: „Odluka o objavljivanju hrvatskih standarada za financijsko izvještavanje“, s Interneta, <http://www.osfi.hr/Uploads/1/2/136/137/1.pdf> , 02.03.2014.

<sup>4</sup> IBID

<sup>5</sup> Mamić, S., I., Posavec, R., S.: „Analiza problema praktične primjene međunarodnih standarada financijskog izvještavanja u Republici Hrvatskoj“, Ekonomski pregled, Vol.63 No.9-10 Listopad 2012.



Primjena MSFI-a propisana je Zakonom o računovodstvu u Republici Hrvatskoj. Naime, obveznici primjene veliki su poduzetnici te poduzetnici čije su dionice ili dužnički vrijednosni papiri uvršteni ili se obavlja priprema za njihovo uvrštavanje na organizirano tržište vrijednosnih papira. Mali i srednji poduzetnici mogu, ako to žele, primjenjivati MSFI-eve u cijelosti izvještavanja.<sup>6</sup>



**Slika 5.1.** Korišteni standardi pri sastavljanju financijskih izvještaja

*Izvor: Empirijsko istraživanje*

Svi operatori koji su sudjelovali u istraživanju imaju obavezu sastavljanja godišnjih financijskih izvještaja, konsolidiranih financijskih izvještaja te podliježu reviziji financijskih izvještaja (Slika 5.2.). Njihove obaveze proizlaze iz Zakona o računovodstvu i reviziji kako je objašnjeno u nastavku. Prema Zakonu o računovodstvu, obveznici sastavljanja godišnjih financijskih izvještaja su poduzetnici i to:<sup>7</sup>

- trgovačka društva i trgovci pojedinci određeni propisima koji uređuju trgovačka društva;

<sup>6</sup> Hrvatska agencija za nadzor financijskih usluga: „Međunarodni računovodstveni standardi i Međunarodni standardi financijskog izvještavanja“, s Interneta, <http://www.hanfa.hr/getfile/39377/Me%C4%91unarodni%20ra%C4%8Dunovodstveni%20standardi%20i%20Me%C4%91unarodni%20standardi%20financijskog.pdf>, 02.03.2014.

<sup>7</sup> Marinčić, I.: „Analiza financijskih izvještaja u trgovačkim društvima“, Ekonomski fakultet u Osijeku, završni rad, Osijek, 2013.

- poslovne jedinice poduzetnika sa sjedištem u stranoj državi ako prema propisima te države ne postoji obveza vođenja poslovnih knjiga i sastavljanja financijskih izvještaja;
- poslovne jedinice iz strane države koji su obveznici poreza na dobit;
- sve pravne i fizičke osobe koje su obveznici poreza na dobit.

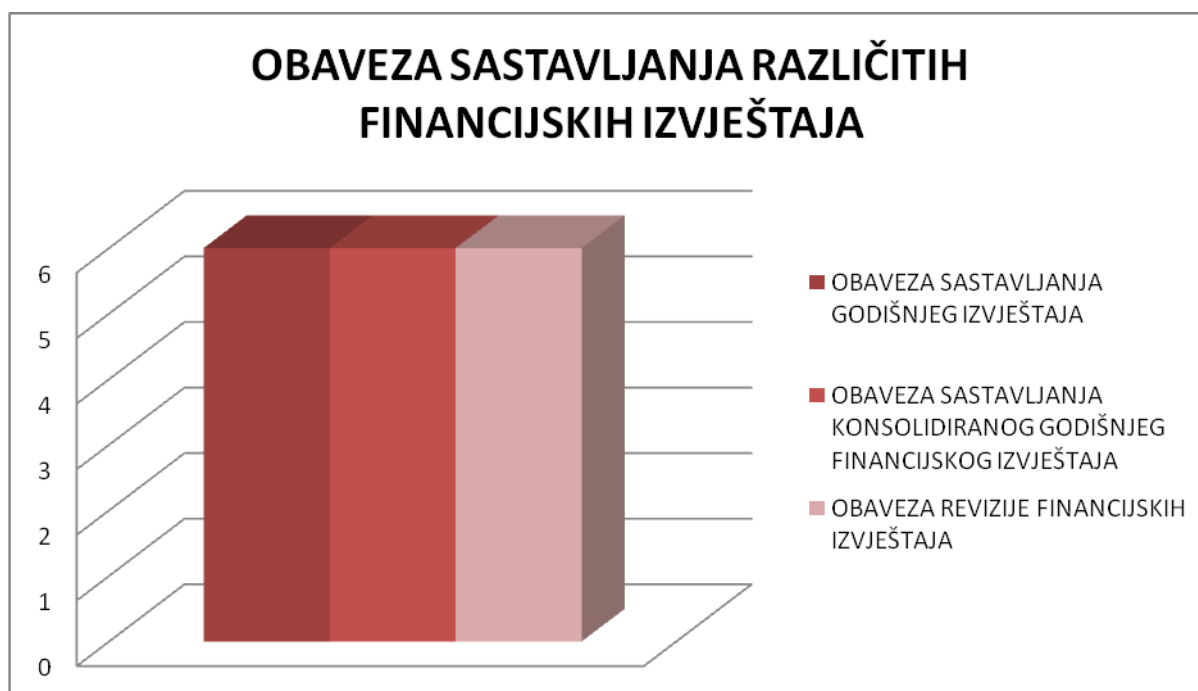
Pri tome su veliki i srednje veliki poduzetnici dužni sastavljati sve propisane financijske izvještaje; bilancu, račun dobiti i gubitka, izvještaj o novčanom toku, izvještaj o promjeni vlasničke glavnice te bilješke uz financijska izvješća, dok mala poduzeća sastavljaju samo bilancu, račun dobiti i gubitka i bilješke. Svrha konsolidacije (spajanje financijskih izvještaja matice i njezinih podružnica) financijskih izvještaja temelji se na potrebama korisnika konsolidiranih financijskih izvještaja. Primarno su to dioničari i vjerovnici matice. Oni su zainteresirani za rezultate poslovanja kao i za financijsku situaciju matice i svih njezinih podružnica kao da se radi o jednom jedinstvenom društvu. Pritom se polazi od osnovne pretpostavke da su konsolidirani financijski izvještaji važniji od temeljnih financijskih izvještaja članova skupine koja se konsolidira. Naime, konsolidirani financijski izvještaji neophodni su radi fer prezentiranja situacije kada jedno trgovačko društvo u grupi ima direktnu ili indirektnu kontrolu nad drugim.<sup>8</sup> Revizija je postupak provjere i ocjene financijskih izvještaja i konsolidiranih financijskih izvještaja obveznika te podataka i metoda koje se primjenjuju pri sastavljanju financijskih izvještaja, na temelju kojih se daje stručno i neovisno mišljenje o istinitosti i objektivnosti financijskog stanja, rezultata poslovanja i novčanih tokova. Reviziji podliježu financijska izvješća.<sup>9</sup>

- velikih poduzetnika (uključuje financijska izvješća osoba iz financijskog sektora),
- srednjih poduzetnika,
- poduzetnika čije su dionice ili dužnički vrijednosni papiri uvršteni ili se obavlja priprema za njihovo uvrštavanje na organizirano tržište vrijednosnih papira te poduzetnici kojima je to određeno posebnim propisima, i
- svih dioničkih društava te komanditnih društava i društava s ograničenom odgovornošću čiji odvojeni, odnosno konsolidirani ukupan prihod u godini koja prethodi reviziji prelazi 30,000.000,00 kuna ako obvezi revizije godišnjih financijskih izvještaja ne podliježu prve tri točke.

---

<sup>8</sup> Gulin, D.: „Kriteriji provođenja i postupci konsolidacije financijskih izvještaja“, s Interneta, <http://web.efzg.hr/dok/RAC/Konsolidacija.pdf> , 02.03.2014

<sup>9</sup> IBID



**Slika 5.2.** Obveze sastavljanja financijskih izvještaja i revizije

*Izvor: Empirijsko istraživanje*

Rezultati upita obveze vođenja troškovnog računovodstva i računovodstvenog odvajanja (Slika 5.3.) ne iznenađuju s obzirom na to da HAKOM te obveze propisuje samo operatorima sa značajnom tržišnom snagom, a takav je samo jedan na području Hrvatske.

Računovodstveno odvajanje (engl. *Accounting separation*, AS) je najčešći instrument koji se koristi za utvrđivanje aktivnosti koje onemogućavaju tržišno natjecanje. Prema navedenom pristupu aktivnosti operatora sa značajnom tržišnom snagom su podijeljene u posebne poslove ili usluge za računovodstvene potrebe. Pritom se, uvođenjem obveze računovodstvenog odvajanja, navedenom operatoru ne nameću pravila niti poželjna organizacija poslovanja, već isključivo sadržaj i oblik prikupljanja računovodstvenih informacija te regulatornog izvještavanja. Kako bi se spriječila diskriminacija na tržištu, te omogućilo praćenje profitabilnosti pojedinih tržišnih segmenata ili usluga koje pruža operator, te olakšalo utvrđivanje međusobnog subvencioniranja, potrebno je također jednoznačno utvrditi cijene, odnosno naknade za transferne usluge između pojedinih segmenata poslovanja operatora sa značajnom tržišnom snagom. Računovodstveno odvajanje će omogućiti nadzor sustavne raspodjele troškova na maloprodajnoj i veleprodajnoj razini.<sup>10</sup>

Prema članku 11 Direktive 2002/19/EC (Pristupna Direktiva) nacionalna regulatorna tijela su obavezna uvesti obvezu računovodstvenog odvajanja određenih djelatnosti vezanih za

<sup>10</sup> Hrvatska agencija za poštu i telekomunikacije: „Računovodstveno odvajanje i troškovno računovodstvo“, konzultacijski dokument, Zagreb, kolovoz 2008, s Interneta, [http://www.hakom.hr/userdocs/images/javnarasprava/Microsoft%20Word%20-%20Računovodstveno%20odvajanje%20i%20troškovno%20računovodstvo\\_Final%20\\_2\\_.pdf](http://www.hakom.hr/userdocs/images/javnarasprava/Microsoft%20Word%20-%20Računovodstveno%20odvajanje%20i%20troškovno%20računovodstvo_Final%20_2_.pdf); 20.02.2013.

međupovezivanje i/ili pristup.<sup>11</sup> Prema Preporuci 2005/698/EC svrha uvođenja računovodstvenog odvajanja jest omogućiti puno višu razinu detalja operativnih troškova i financijskih rezultata za različita tržišta i usluge od onih dobivenih zakonskim financijskim izvještajima operatora sa značajnom tržišnom snagom.<sup>12</sup> Operator sa značajnijom tržišnom snagom može narušavati načelo jednakih tržišnih uvjeta na više načina, kao što su previsoke cijene veleprodajnih usluga, diskriminacija pri određivanju cijena, međusobno subvencioniranje te predatorsko određivanje cijena. Takav operator na ove načine može ograničiti konkurenciju i spriječiti ulazak novih operatora na tržište. Računovodstveno odvajanje je najčešći instrument koji se koristi za utvrđivanje aktivnosti koje onemogućavaju tržišno natjecanje. HAKOM u skladu sa ZEK-om može odrediti operatorima obvezu računovodstvenog razdvajanja određenih djelatnosti u vezi s međupovezivanjem i/ili pristupom. Prema navedenom pristupu, aktivnosti takvog operatora su podijeljene u posebne poslove ili usluge za računovodstvene potrebe. Uvođenje obveze računovodstvenog odvajanja nadopunjuje obveze transparentnosti i nediskriminacije, s obzirom da podaci dobiveni kao rezultat računovodstvenog odvajanja trebaju vjerno održavati poslovanje određenih dijelova operatora sa značajnijom tržišnom snagom kao da se radi o zasebnim poslovnim subjektima. Kako bi se spriječila diskriminacija na tržištu, omogućilo praćenje profitabilnosti pojedinih tržišnih segmenata ili usluga koje pruža takav operator, te olakšalo utvrđivanje međusobnog subvencioniranja, potrebno je također jednoznačno utvrditi cijene, odnosno naknade za transferne usluge, tzv. transferne cijene, između pojedinih segmenata poslovanja unutar takvog operatora. Računovodstveno odvajanje će omogućiti nadzor sustavne raspodjele troškova na maloprodajnoj i veleprodajnoj razini te onemogućiti prevaljivanje troškova i prelijevanje prihoda.<sup>13</sup> Nametanje obaveze računovodstvenog odvajanja je doprinos transparentnosti i nediskriminacijskim obavezama, jer ta obveza navodi da izvještaji dobiveni računovodstvenim odvajanjem trebaju prikazivati što bolje izvršenje svih dijelova poslovanja operatora sa značajnom tržišnom snagom odnosno prikazati poslovanje toliko detaljno kao da poslovanje vodi pojedinačno. Računovodstveno odvajanje će, u slučaju vertikalno integriranih poduzeća, spriječiti diskriminaciju vlastitih poslovnih aktivnosti u odnosu na druge operatore na tržištu, te međusobno subvencioniranje koje nije u skladu s tržišnim principima.<sup>14</sup> Prema Članku 11 Pristupne Direktive potrebno je osigurati suglasnost s ciljanim poduzećem odnosno operatorom s značajnom tržišnom snagom, koji je obveznik računovodstvenog odvajanja i

---

<sup>11</sup> Direktiva 2002/19/EC Europskog Parlamenta i Vijeća 7. ožujka 2002 na temu pristupa, interkonekcije i elektroničkih komunikacijskih mreža i povezanih usluga (Pristupna Direktiva), s Interneta, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0019:EN:HTML>; 20.02.2013.

<sup>12</sup> Službene novine Europske Unije, Komisijska Preporuka 2005/698/EC 19. rujna 2005 na temu računovodstvenog odvajanja i troškovnog računovodstva pod regulatornim okvirom elektroničkih komunikacija, s Interneta, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:266:0064:0069:EN:PDF>; 20.02.2013.

<sup>13</sup> Hrvatska agencija za poštu i telekomunikacije: „Računovodstveno odvajanje i troškovno računovodstvo“, konzultacijski dokument, Zagreb, kolovoz 2008, s Interneta, [http://www.hakom.hr/userdocsimages/javnarasprava/Microsoft%20Word%20-%20Racunovodstveno%20odvajanje%20i%20troskovno%20racunovodstvo\\_Final%20\\_2\\_.pdf](http://www.hakom.hr/userdocsimages/javnarasprava/Microsoft%20Word%20-%20Racunovodstveno%20odvajanje%20i%20troskovno%20racunovodstvo_Final%20_2_.pdf); 20.02.2013.

<sup>14</sup> Ibid.

troškovnog računovodstva, kako bi imao transparentne veleprodajne i unutarnje transferne cijene. Nadalje, prema Preporuci, obaveza računovodstvenog odvajanja nametnuta operatoru sa značajnom tržišnom snagom može obuhvatiti i tržište na kojem spomenuti operator ima značajnu tržišnu snagu ali i ono na kojem nema (kako bi se osigurala usklađenost podataka).<sup>15</sup> Prema članku 11 Pristupne direktive, regulator može specificirati i format i računovodstvenu metodologiju koju će koristiti operator koji ima obavezu vođenja troškovnog razdvajanja i troškovnog računovodstva. Prema Preporuci, računovodstveno odvajanje podrazumijeva razdvajanje troškova, angažiranog kapitala i prihoda. Prema članku 13 Pristupne Direktive, bez obzira na redovite podatke nastale obavezom računovodstvenog razdvajanja, regulator također može zahtijevati i ad hoc pripremu računovodstvenih podataka kako bi se olakšala verifikacija suglasnosti s obavezom transparentnosti i nediskriminacije.<sup>16</sup> Računovodstveno odvajanje i troškovno računovodstvo su usko vezani, te oboje imaju za cilj služiti transparentnosti i nediskriminaciji. Tako, svaka propisana metodologija troškovnog računovodstva ili računovodstvenog odvajanja koja se koristi kao temelj za kontrolu cjenovnih odluka treba biti određena na način da potiče učinkovite investicije, identificira potencijalna protu konkurentna ponašanja te je u skladu s ciljevima regulatorne politike navedenim u Direktivi 2002/21/EC (Okvirna Direktiva). Prema Preporuci Komisije 19. rujna 2005. godine (2005/698/EC) preporučeno je da regulator zahtijeva razdvajanje operativnih troškova, angažiranog kapitala i prihoda na razini potrebnoj za ostvarenja načela transparentnosti i regulatornih ciljeva koje propisuje nacionalno pravo ili Pravo zajednice (Zajednica EU). Nadalje, raspodjela troškova, kapitala i prihoda će biti u skladu sa načelom troškovne uzročnosti (npr. *Activity-Based Costing*, ABC), koja se može koristiti u troškovnom računovodstvu i također u troškovnom razdvajanju.<sup>17</sup> Sustavi troškovnog računovodstva i računovodstvenog razdvajanja operatora sa značajnom tržišnom snagom bi trebali isporučivati regulatorne financijske informacije koje osiguravaju usklađenost sa regulatornim obvezama: relevantnost, pouzdanost, usporedivost i materijalnost. Prema Preporuci, regulatorni financijski izvještaji ovlaštenog operatora trebaju biti objavljeni te revidirani godišnje kako si se osigurala dosljednost s principima obveze računovodstvenog razdvajanja. Prema Direktivi 2002/22/EC (Direktiva o univerzalnim uslugama) reviziju će obavljati kvalificirano tijelo, neovisno o ovlaštenom operatoru. U slučaju da regulator ima potrebno kvalificirano osoblje, reviziju može napraviti i on sam. Izvještaj vezan za dosljednost treba biti objavljen godišnje,

---

<sup>15</sup> Direktiva 2002/19/EC Europskog Parlamenta i Vijeća 7. ožujka 2002 na temu pristupa, interkonekcije i elektroničkih komunikacijskih mreža i povezanih usluga (Pristupna Direktiva), s Interneta, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0019:EN:HTML>; 20.02.2013.

<sup>16</sup> Ibid.

<sup>17</sup> Službene novine Europske Unije, Komisijaska Preporuka 2005/698/EC 19. rujna 2005 na temu računovodstvenog odvajanja i troškovnog računovodstva pod regulatornim okvirom elektroničkih komunikacija, s Interneta, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:266:0064:0069:EN:PDF>; 20.02.2013.

te treba obratiti pozornost kako se ne bi objavili osjetljivi podaci ovlaštenog operatora.<sup>18</sup> Prema Preporuci, kada regulator revidira sustav troškovnog računovodstva ovlaštenog operatora, treba obratiti posebnu pozornost na sposobnost sustava da analizira i prikaže troškovne podatke, posebice sposobnost razlikovanja direktnih i indirektnih troškova.

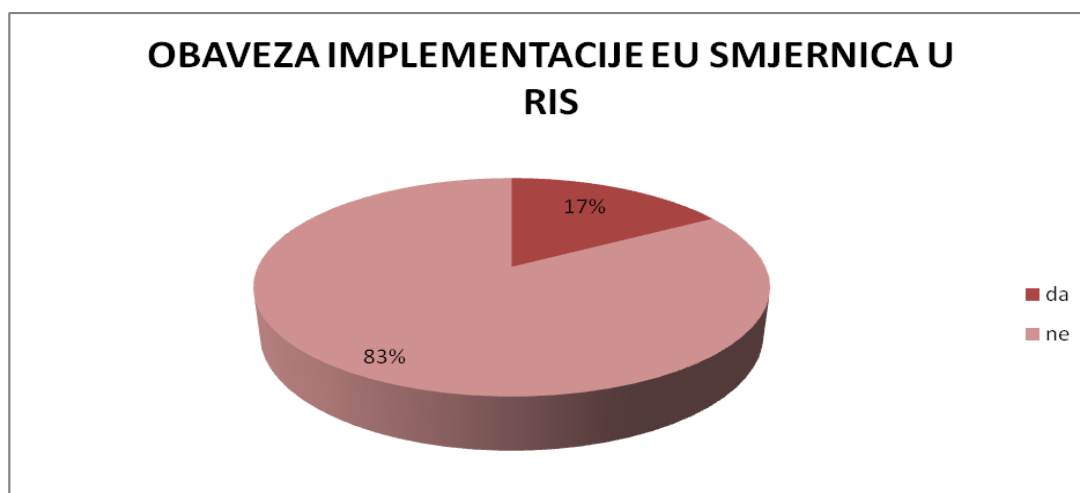


**Slika 5.3.** Obaveza računovodstvenog odvajanja i troškovnog računovodstva

*Izvor: Empirijsko istraživanje*

Na upit „Da li se u računovodstveni informacijski sustav (RIS) Vašeg poduzeća implementiraju smjernice Europske komisije, neovisno o tome je li Vaše poduzeće njihov obveznik ili ne?“ samo je jedan operator odgovorio potvrdno (Slika 5.4.) što ne iznenađuje s obzirom na to da nitko nema obvezu implementacije istih osim operatora sa značajnom tržišnom snagom što propisuje HAKOM.

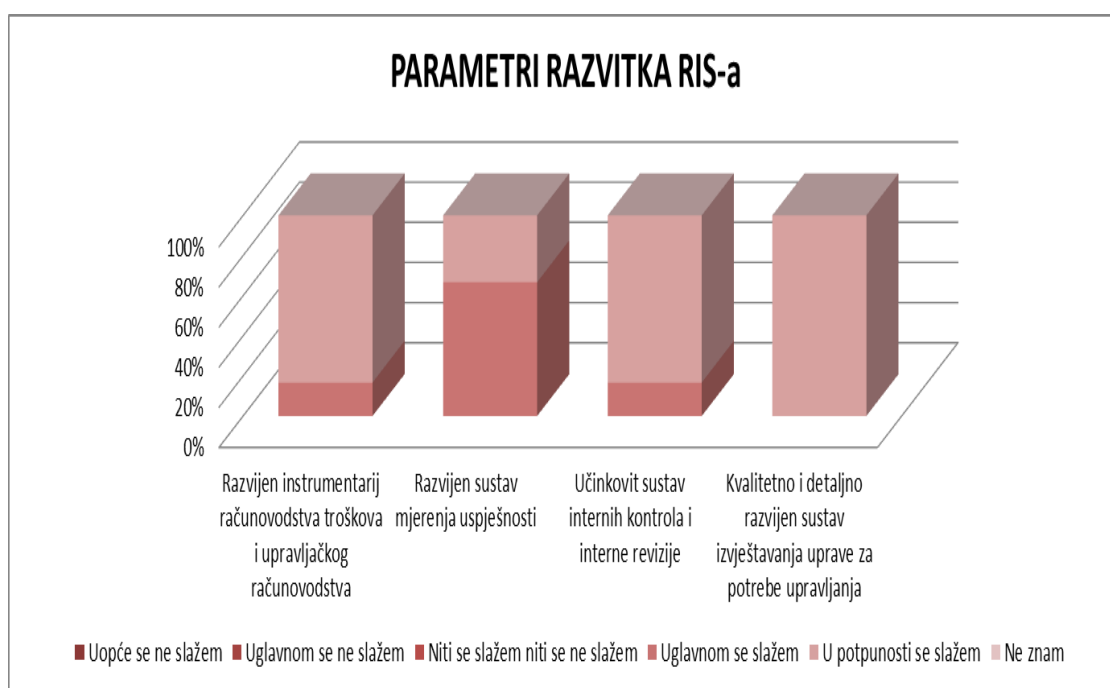
<sup>18</sup> Direktiva 2002/22/EC Europskog Parlamenta i Vijeća 7. ožujka 2002. o univerzalnim uslugama i pravima korisnika vezanih za elektroničke komunikacijske mreže i usluge (Direktiva Univerzalne Usluge), s Interneta, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:108:0051:0051:EN:PDF>, 20.02.2013.



**Slika 5.4.** Implementacija EU smjernica u RIS-u poduzeća

*Izvor: Empirijsko istraživanje*

Slika 5.5. otkriva kako postojeći RIS-ovi tele operatora koji posluju na području Hrvatske imaju ili u potpunosti ili uglavnom razvijen instrumentarij računovodstva troškova i upravljačkog računovodstva, razvijen sustav mjerenja uspješnosti, učinkovit sustav internih kontrola i interne revizije te kvalitetno i detaljno razvijen sustav izvještavanja uprave za potrebe upravljanja.



**Slika 5.5.** Parametri razvitka RIS-a

*Izvor: Empirijsko istraživanje*

Prije same analize i podjele troškova, bitno je objasniti razlike u rashodima, izdancima i troškovima kao osnovnim ekonomskim kategorijama. Troškovi su nužna ulaganja učinjena u

svrhu postizanja učinaka (proizvodnju proizvoda, obavljanje usluga, nabavu trgovačke robe).<sup>19</sup> Troškovi su novčani izraz utroška sirovina, materijala, postrojenja i opreme, alata i pogonskog inventara, usluga drugih, plaća i nadnica koji nastaju u poslovanju. Vrijednost učinaka (proizvoda, usluga) izražena je kroz iznos troškova koji su nastali u svezi sa stvaranjem tih učinaka.<sup>20</sup>

Rashodi su smanjenje ekonomskih koristi kroz obračunsko razdoblje u obliku odljeva ili smanjenja sredstava ili stvaranja obveza, što za posljedicu ima smanjenje glavnice, osim onog u svezi s raspodjelom glavnice sudionicima.<sup>21</sup> Rashod je, negativnog predznaka, komponenta rezultata poslovanja koja se sučeljava s prihodima, pozitivnog predznaka, istog obračunskog razdoblja u cilju utvrđivanja rezultata poslovanja promatranog obračunskog razdoblja.<sup>22</sup>

Pojam izdatka se vezuje uz smanjenje novčanih sredstava tj. odljev novca iz poslovnog subjekta. Izdatak može nastati prije nastanka troška, u isto vrijeme kad i trošak ili nakon nastanka troška. Novčani izdatak također ne mora biti povezan sa nastankom troška. Trošak se uvijek evidentira onda kada je nastao, a ne kada je uslijedio izdatak za njegovo podmirenje. Samo kvantitativna definicija troška glasi da je to umnožak utroška i cijene troška.<sup>23</sup> Odnosno, kako je već rečeno, trošak je novčano izraženi utrošak. Utrošak se izražava neutralnim jedinicama, a trošak novčanim jedinicama.

Općenito gledajući trošak je širi pojam od rashoda, budući da rashodi predstavljaju samo dospjele troškove. Svi troškovi u trenutku nastajanja ne postaju odmah rashodi. To je posljedica primjene jednog od osnovnih računovodstvenih načela, a to je načelo povijesnog troška (načelo nabavne vrijednosti). Prema tom načelu, cjelokupna imovina poslovnog subjekta početno se u računovodstvu evidentira po trošku nabave. Imovina koja se nabavlja u računovodstvu se iskazuje po njezinom trošku nabave koji obuhvaća sve troškove koji su bili potrebni da bi se ista nabavila.<sup>24</sup> Zalihe proizvodnje i gotovih proizvoda, tj. imovina odnosno učinci koji se proizvode, iskazuje se po trošku proizvoda (troškovima proizvodnje) koji obuhvaća sve troškove nastale radi proizvodnje proizvoda. Troškovi nabave i troškovi proizvoda (proizvodnje) predstavljaju troškove koji se u trenutku nastanka iskazuju kao

---

<sup>19</sup> Žager, K., Tušek, B., Vašiček, V., Žager, L.: "Osnove računovodstva", Hrvatska zajednica računovođa i financijskih djelatnika, Zagreb, 2007.

<sup>20</sup> Ibid.

<sup>21</sup> Gulin, D.: „Raspoređivanje općih troškova proizvodnje na mjesta i nositelje troškova“, Računovodstvo i financije br. 8/1998.

<sup>22</sup> Lutitsky, D., I., Gulin, D., Saćer, M., I., Tadijančević, S., Tušek, B., Vašiček, V., Žager, K., Žager, L.: "Računovodstvo", Hrvatska zajednica računovođa i financijskih djelatnika, Zagreb, 2010.

<sup>23</sup> Ibid.

<sup>24</sup> Perčević, H.: „Utjecaj računovodstvenih metoda alokacije troškova proizvodnje na ocjenu profitabilnosti proizvoda“, magistarski rad obranjen 14.10.2005., Ekonomski fakultet Zagreb.



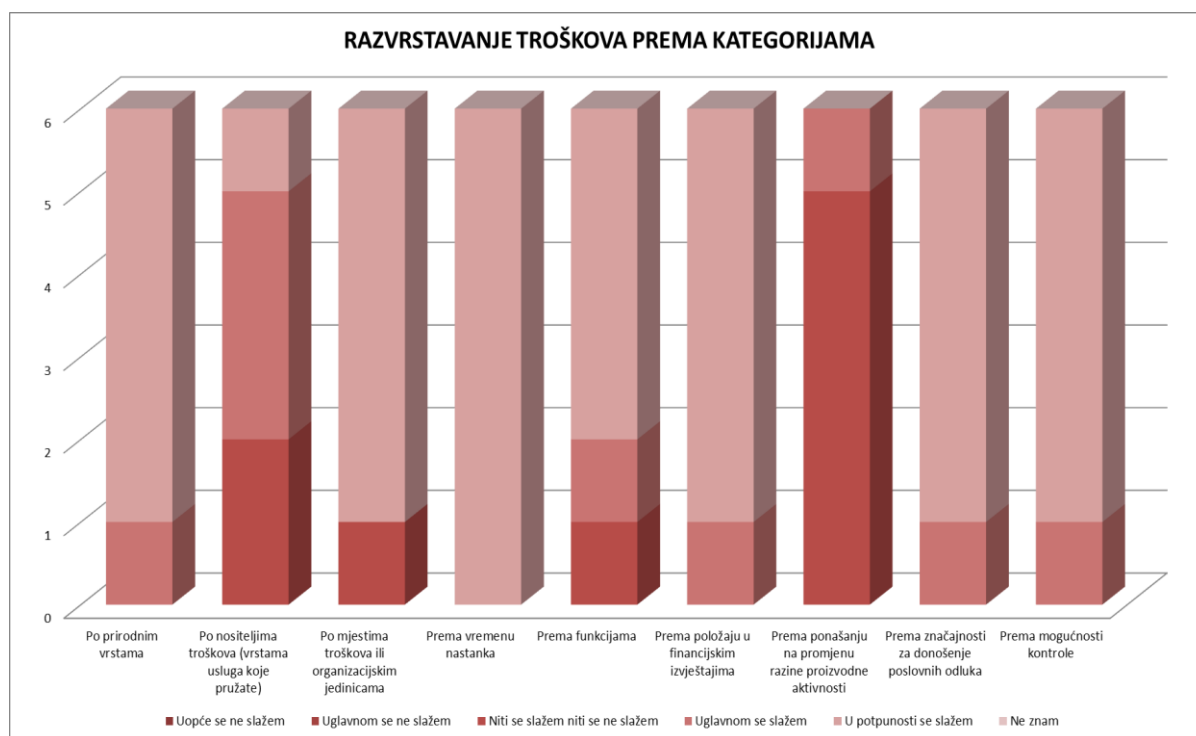
imovina i prezentiraju u bilanci poslovnog subjekta. U računovodstvenoj terminologiji takvi troškovi nazivaju se nedospjeli troškovi ili kapitalizirani troškovi, jer se od njih očekuju buduće ekonomske koristi. Nedospjeli troškovi postaju rashodi tek u onom obračunskom razdoblju u kojem se imovina na koju se odnose proda, uništi, daruje ili na neki drugi način otuđi, kao što su manjkovi ili krađe odnosno kad se od nje više ne očekuju buduće ekonomske koristi. Tada nedospjeli troškovi postaju dospjeli i iskazuju se kao rashodi te se sučeljavaju s prihodima istog obračunskog razdoblja i iskazuju u izvještaju o dobiti. Osim ovih troškova u dospjele troškove uključuju se i svi administrativni troškovi uprave i prodaje (troškovi razdoblja) koji nastaju u tijeku razdoblja, a ne uključuju se u troškove nabave imovine i ne mogu se vezati uz troškove proizvodnje proizvoda niti se ne mogu iskazivati kao imovina u bilanci poslovnog subjekta. Takvi troškovi su rashodi razdoblja u kojem nastaju i nadoknađuju se iz prihoda istog obračunskog razdoblja. Dakle, na kraju svi troškovi postaju rashodi, samo je pitanje kada, odnosno u kojem vremenu ili kojem obračunskom razdoblju.

Rashodi se dijele na redovne i izvanredne. Redovni rashodi dijele se na poslovne i financijske rashode. Izvanredni rashodi su oni rashodi koji se ne pojavljuju učestalo u poslovanju poslovnog subjekta te se ne mogu predvidjeti, ne dovode do stvaranja novih vrijednosti, a uzrokuju smanjenje novca ili povećanje obveza. Poslovni rashodi predstavljaju rashode koji nastaju u svezi s obavljanjem redovne poslovne aktivnosti poslovnog subjekta, a obuhvaćaju najčešće troškove prodanih proizvoda, troškove nabave prodane robe, troškove prodaje i administrativne troškove. Poslovni rashodi su dakle troškovi. Financijski rashodi su rashodi vezani uz korištenje novčanih sredstava, a obuhvaćaju najčešće rashode od kamata i negativne tečajne razlike.

Kako je i očekivano, svi odnosno velika većina operatora iskazuju svoje troškove prema sljedećim kategorijama: (Slika 5.6.)

- Po prirodnim vrstama,
- Po mjestima troškova ili organizacijskim jedinicama,
- Prema vremenu nastanka,
- Prema funkcijama,
- Prema položaju u financijskim izvještajima,
- Prema značajnosti za donošenje poslovnih odluka i
- Prema mogućnosti kontrole.

Kategorija razvrstavanja troškova „Po nositeljima troškova (vrstama usluga koje se pružaju)“ se uglavnom koristi od strane operatora dok je većina indiferentna prema kategoriji razvrstavanja troškova „Prema ponašanju na promjenu razine proizvodne aktivnosti“. Može se zaključiti da veliki dio varijabilnih troškova ne varira s količinom proizvodnje, već s nekom aktivnošću koja se ne pojavljuje kao output proizvodnje (npr. aktivnost osiguranja kvalitete proizvoda koja je zasigurno jedna od najbitnijih aktivnosti telekomunikacijskih operatora s obzirom na specifične usluge koje pružaju).



**Slika 5.6.** Razvrstavanje troškova prema kategorijama

*Izvor: Empirijsko istraživanje*

Tradicionalan pristup metodi raspodjele troškova sastoji se od tri osnovna koraka: akumulacija troškova u okviru proizvodnog ili neproizvodnog odjela; raspoređivanje troškova neproizvodnog odjela ka proizvodnim odjelima; i raspoređivanje krajnjih (revidiranih) troškova proizvodnog odjela ka različitim proizvodima, uslugama ili klijentima. Troškovi dobiveni ovakvim tradicionalnim pristupom trpe nekoliko nedostataka koji mogu rezultirati iskrivljenim troškovima koji se koriste u svrhu donošenja odluke. Na primjer, tradicionalan pristup raspodjeljuje trošak praznog kapaciteta ka proizvodima. Shodno tome, takvim se proizvodima zaračunavaju troškovi sredstava koja nisu koristili. Kako bi se otklonio ovaj nedostatak, mnoge su kompanije posegle za novim rješenjem odnosno drugačijim pristupom metodi raspodjele troškova kao što je ABC metoda raspodjele troškova koja se najčešće koristi u sklopu FAC računovodstvene metodologije, ali se može i u sklopu LRIC metodologije, ili metoda troškovno-volumnog odnosa (engl. *Cost Volume Relationship*, CVR) i Shapley Shubik metoda raspodjele troškova u sklopu LRIC računovodstvene metodologije. Tradicionalna metoda direktne troškove pripisuje troškovnim objektima- uslugama. Ti troškovi su direktno pripisani pojedinim uslugama koje su uzrokuju nastanjenje istih. Glavni problem svake troškovne metode je raspodjela indirektnih troškova. Razlog tomu leži u činjenici da se ti troškovi ne mogu direktno izjednačiti sa pojedinom uslugom, već moraju biti raspodijeljeni na nekoj opravdanoj bazi koja točno prikazuje odnos između indirektnih troškova i određene usluge. Ovaj odnos je često veoma teško izraziti koristeći samo jednu bazu raspodjele. Važno je istaknuti da ne postoji baza koja bi mogla osigurati točnu raspodjelu indirektnih troškova na usluge. Izabrana troškovna baza može biti više ili manje

točna, ali ne može biti 100% točna. Indirektni troškovi u tradicionalnoj metodi se najčešće dodjeljuju uslugama koristeći slijedeće troškovne baze raspodjele:<sup>25</sup>

- a) direktni sati rada,
- b) ukupni direktni troškovi,
- c) minute, itd.

Indirektni troškovi se pripisuju troškovnim objektima prema dodatnoj stopi raspodjele koja se izračunava na izabranoj troškovnoj bazi raspodjele.

Na pitanje „Da li ste upoznati s ABC metodom, i ako da, da li bi je uveli u računovodstveni informacijski sustav Vašeg poduzeća?“ (Slika 5.7.) svi operatori su odgovorili potvrdno, što i ne čudi s obzirom na prednosti koje donosi implementacija ABC metode u računovodstveni informacijski sustav poduzeća.



**Slika 5.7.** Pristanak uvođenja ABC metode u RIS

*Izvor: Empirijsko istraživanje*

ABC metoda je osmišljena s ciljem ispravka svih nedostataka koje je imala tradicionalna metoda. Ista je inicijalno osmišljena kako bi metoda raspodjele troškova postala pravedna i točna, a samim time i vrednovanje proizvodne profitabilnosti upravo zbog povećanja indirektnih troškova. Sukladno tome, ABC metoda fokusira pažnju na indirektno troškove. Svrha joj je definirati način koji bi najviše odgovarao raspodjeli indirektnih troškova na troškovne objekte. Glavna pretpostavka ABC metode je da proizvodi koriste aktivnosti, a aktivnosti koriste resurse. Što je veći broj aktivnosti potreban, to je ABC metoda kompleksnija. Aktivnost se definira kao svaki događaj, postupak, prijenos ili djelovanje koji

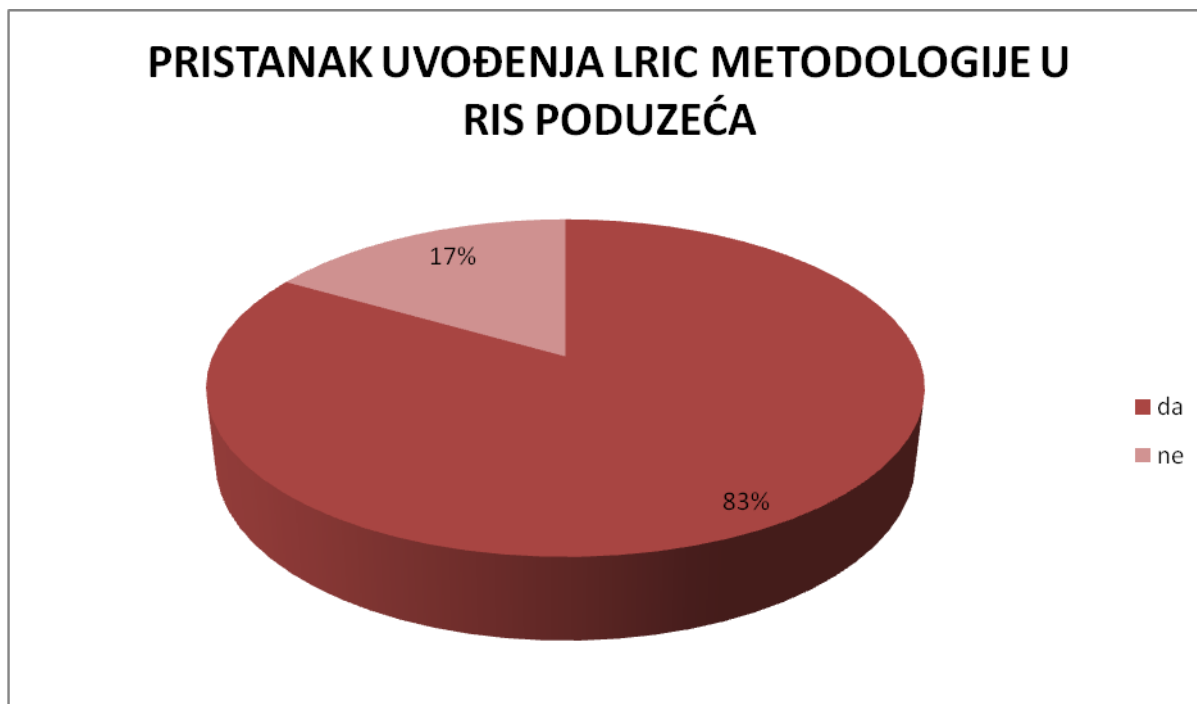
<sup>25</sup> Dražić Lutitsky, I., Broz Tominac, S., Ivić, M. (2011): „Activity based system in telecommunications industry“, 19<sup>th</sup> International Conference on Software Telecommunications and Computer Networks, Split-Hvar-Dubrovnik, 15.-17. rujana 2011, ISBN 978-953-290-027-9.

za ishod ima nastajanje troška pri proizvodnji proizvoda ili pružanju usluge.<sup>26</sup> ABC metoda također direktne troškove locira na proizvode ili usluge, tako da je glavna pozornost usmjerena na indirektno troškove koji se raspodjeljuju na aktivnosti umjesto odjele (što je slučaj kod tradicionalne metode). Načelno, primjena ABC metode se odvija u dvije faze. U prvoj se fazi indirektni troškovi se raspodjeljuju na *troškovni bazen po aktivnostima* (engl. *Activity Cost Pool, ACP*). Važno je odrediti ovisnost između određenog indirektnog troška i identificirane aktivnosti. Svaki indirektni trošak mora biti pripisan odgovarajućoj aktivnosti koja uzrokuje njegov nastanak. U drugoj se fazi indirektni troškovi pridružuju proizvodima iz *ACP-a* koristeći definirani troškovni pokretač (engl. *Cost Driver*). Troškovni pokretač je svaki faktor ili aktivnost koji ima direktno uzročno posljedičnu vezu sa utrošenim resursima [4]. ABC metoda koristi višestruke troškovne baze raspodjele kako bi pridružila indirektno troškove uslugama ili proizvodima. Uporaba takvih baza može pružiti točnije i objektivnije profitno vrednovanje. Troškovni pokretač bi trebao pravilno prikazati odnos između određene aktivnosti i troškovnih objekata. Ako ne, čak i ova troškovna metoda može odvesti ka troškovnom iskrivljenju i nepouzdanim profitnom vrednovanju. ABC metoda je veoma kompleksna i potrebno je mnogo vremena, truda i sredstava kako bi se ista implementirala. Njezina je implementacija opravdana jedino u slučaju kad koristi iste premašuju troškove implementacije. Dakle, menadžment kompanije pri odlučivanju o implementaciji ABC metode mora biti siguran da će mu ABC metoda omogućiti korisnije troškovne informacije za donošenje poslovnih odluka od onih koji bi mu pružila tradicionalna metoda.

Odgovor na pitanje „Da li ste upoznati s LRIC metodologijom, i ako da, da li bi je uveli u informacijski sustav Vašeg poduzeća?“ nije bio jednoglasan kao na prethodno, međutim iznenađuje da su svi operatori upoznati sa LRIC metodologijom s obzirom na to da se radi o novoj metodologiji koja se koristi za sastavljanje financijskih izvještaja čiju obvezu primjene imaju samo operatori sa značajnom tržišnom snagom a takav je samo jedan na području Hrvatske. S druge strane gledano, potvrdni odgovori otkrivaju praćenje rada HAKOM-a i smjernica koje uvodi EU iako još ne postoji obveza implementacije istih po pitanju LRIC metodologije.

---

<sup>26</sup> Dražić Lutitsky, I., Ivić, M. (2013): „Valuation of long-term tangible asset under LRIC methodology“, 12<sup>th</sup> International Conference on Telecommunications, Zagreb, 26.-28. lipnja 2013, ISBN 958-953184-176-4.



**Slika 5.8.** Pristanak uvođenja LRIC metodologije u RIS poduzeća

*Izvor: Empirijsko istraživanje*

LRIC računovodstvena metodologija je relativno nova metodologija za raspoređivanje troškova u telekomunikacijskoj industriji koju koriste isključivo i samo telekomunikacijska poduzeća. Literarni pregled na temu LRIC-a je skroman i sadrži većinom konzultacijske dokumente zahvaljujući konzultantskim poduzećima koje se bave spomenutom metodologijom te problemima koje donosi. Troškovno modeliranje telekomunikacijskih mreža se bazira na troškovnoj uzročnosti i mrežnoj iskorištenosti svake omogućene usluge.

Modeliranje na temelju dugoročnih inkrementalnih troškova (LRIC) je ekonomski pristup troškovne metodologije koji se često koristi u telekomunikacijama zato što je dobro prilagođen industrijama u kojima se ostvaruju znatna ulaganja. Može se definirati kao dugoročni trošak za pružanje definiranog „inkrementa“ usluge. Smjernice Europske regulatorne grupe<sup>27</sup> iz 2005. za implementaciju, Preporuka Komisije o računovodstvenom odvajanju i sustavima troškovnog računovodstva, navode: „Konceptualno,LRIC metodologija izračunava trošak pružanja definiranog inkrementa izlaznog proizvoda, na temelju budućih troškova učinkovitog operatora. Kod primjene dugoročne perspektive svi se troškovi (uključujući kapitalna ulaganja), smatraju varijabilnima (ili se mogu izbjeći). LRIC stoga predstavlja metodologiju prema kojoj se troškovi na kapitalno intenzivnom tržištu elektroničkih komunikacija, koje na veleprodajnoj razini karakteriziraju značajni troškovi

<sup>27</sup> The Independent Regulators Group: „ERG COMMON POSITION: Guidelines for implementing the Commission Recommendation C (2005) 3480 on Accounting Separation & Cost Accounting Systems under the regulatory framework for electronic communications“, s Interneta,[http://www.erg.eu/streaming/erg\\_05\\_29\\_erg\\_cp\\_rec\\_as\\_and\\_cas\\_final.pdf?contentId=543322&field=ATTACHED\\_FILE](http://www.erg.eu/streaming/erg_05_29_erg_cp_rec_as_and_cas_final.pdf?contentId=543322&field=ATTACHED_FILE)25.01.2012.

ulaganja i dugi vijek trajanja imovine, mogu analizirati i koristiti za određivanje cijena na troškovno orijentiran način.<sup>28</sup>

LRIC metodologija, katkada zvana i LRAIC (engl. *Long Run Average Incremental Costs*, LRAIC) metodologija, procjenjuje dodatne troškove nastale proizvodnjom usluge, zavisne o troškovima koji su već nastali proizvodnjom portfelja drugih usluga. Inkrementalni trošak jedne usluge ili proizvoda na neki način predstavlja troškovno sniženje (troškovnu uštedu) koja je rezultat ne proizvodnje odnosno ne pružanja iste. Drugim riječima, trošak nastao proizvodnjom tog jednog dodatnog proizvoda ili usluge koji nije dio planiranog portfelja proizvoda ili usluga naziva se inkrementalni trošak.<sup>29</sup> Dugoročan koncept obuhvaća uzimanje troškova nastalih u dugoročnoj perspektivi. U dugom roku proizvodni fiksni troškovi se smatraju varijabilnim troškovima. Dugoročni inkrementalni troškovi jednog proizvoda ili usluge dakle predstavljaju sve troškove koji su mogli biti izbjegnuti da taj jedan proizvod odnosno usluga nije bio proizveden. Dakle, inkrementalni troškovi uključuju sve troškove koji se direktno mogu pripisati tome jednom proizvodu ili usluzi, bez obzira jesu li u strogom smislu varijabilni (ovisno o nivou prometa na zadanom kapacitetu) ili fiksni (čine kapacitet). Međutim, taj jedan proizvod ili usluga može koristiti zajedničkim spajanjem s drugim proizvodima ili uslugama. Inkrementalni troškovi (čak i dugoročni, strogo govoreći) uzimaju u obzir samo dio troškova u slučaju združenih troškova (razmjerno njihovoj učestalosti), ali ne i zajedničkih troškova. Inkrementalni troškovi su važni pri odlučivanju o proizvodnji dodatne jedinice proizvoda ili usluge. Najčešće, menadžment poduzeća očekuje da će prihodi od prodaje te dodatne jedinice nadmašiti troškove proizvodnje iste, te omogućiti veći prihod od kapitala nego što je trošak kapitala. Postoji niz različitih mjera LRIC-a koje se mogu koristiti, a ključna razlika je u definiciji inkrementa.

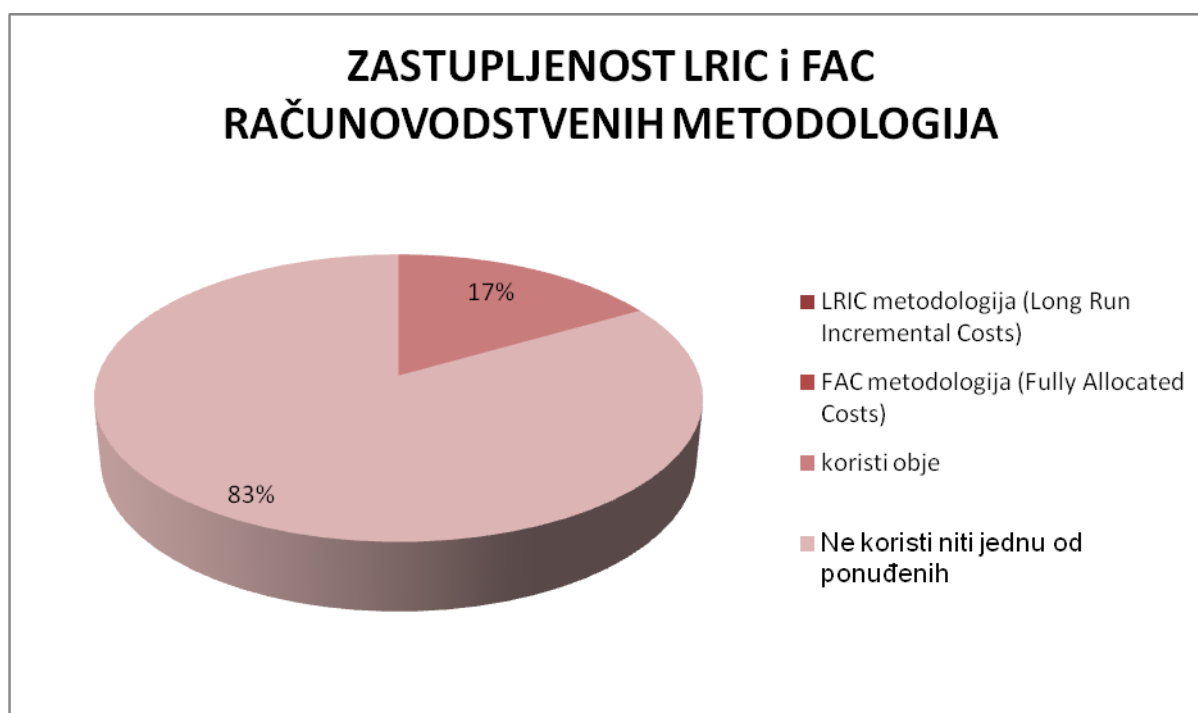
Kad se govori o zastupljenosti FAC i LRIC metodologija u računovodstvenim informacijskim sustavima tele operatora u Hrvatskoj, samo jedan koristi obje metodologije dok ostali koriste druge (Slika 5.9.). Daje se zaključiti da većina operatora nema implementiranu ABC metodu (samo dva od šest ispitanika) i LRIC metodologiju (samo jedan od šest ispitanika) u svoj RIS, što i ne čudi s obzirom da je implementacija ABC metode skupa i komplicirana, a obvezu primjene LRIC metodologije pri sastavljanju financijskih izvještaja ima samo jedan operator na području Hrvatske. Na pitanje koje druge metodologije koriste, dobivena su samo dva odgovora a ona su sljedeća: „Sustav je ograničen te se raspodjela vrši u excelu, ovisno o tipu izvještaja.“ i „Value-based management“. Prvi odgovor otkriva da se radi o malenom operatoru čiji je sustav raspodjele troškova jednostavan pa nema potrebe niti obveze uvođenja spomenutih metodologija.

---

<sup>28</sup> Ibid.

<sup>29</sup> Um, P. N., Gille, L., Simon, L. & Rudelle, C.: „A Model for Calculating Interconnection Costs in Telecommunications“, The World Bank, 2004., ISBN 0-8213-5671-2.

Drugi odgovor je menadžment temeljen na vrijednosti (engl. *Value-based management*, VBM) koji se odnosi na poslovni pristup koji uvijek u središte pozornosti stavlja vrijednosti (maksimiziranje vrijednosti za vlasnike). Unutar ove metodologija se koristi ABC metoda koja osigurava preciznije mjerenje profitabilnosti i stvaranje ekonomske vrijednosti po proizvodima, pogonima, procesima i slično. Financijski izvještaji ponekad „iskrive“ ili ne daju dosljednu predodžbu o ekonomskom stanju poslovanja. VBM predstavlja okvir za donošenje odluka koji egzaktno kombinira financijske i strateške odluke kako bi se mogao slijediti cilj maksimalnog stvaranja vrijednosti. Koncept naglašava analizu novčanog tijeka na dugi rok i analizu rizičnosti menadžerskih odluka. Zadatak mu je procijeniti i utvrditi ekonomsku vrijednost strategije poslovanja.<sup>30</sup>



**Slika 5.9.** Zastupljenost LRIC i FAC računovodstvenih metodologija

*Izvor: Empirijsko istraživanje*

Samo jedan operator koristi kao bazu tekuće troškove u RIS-u dok ostali koriste povijesne troškove, što se može vidjeti na Slici 5.10. Povijesni trošak (trošak stjecanja) najstarije je načelo procjene koje se primjenjuje pri početnom vrednovanju svih pozicija imovine i obveza. Osnovna prednost načela troška u odnosu prema ostalim načelima jest to što se može lako utvrditi i dokazati računovodstvenim ispravama o već nastalim događajima i transakcijama. Osnovna slabost tog načela je gubljenje realnosti pozicija financijskih izvještaja prilikom promjena cijena odnosno vrijednosti između početnoga i svakog naknadnog vrednovanja

<sup>30</sup> Dunković, D.: „Strateško menadžersko računovodstvo“, s Interneta, [http://bib.irb.hr/datoteka/443463.Skripta\\_RRiF\\_SMR\\_s\\_vjezbama\\_2011.pdf](http://bib.irb.hr/datoteka/443463.Skripta_RRiF_SMR_s_vjezbama_2011.pdf), 02.03.2014.

imovine i obveza.<sup>31</sup> To načelo je prikladno za onaj dio imovine tele operatora čija se tržišna vrijednost ne mijenja svakodnevno, dok bi se načelo tekućeg troška trebalo primjenjivati za onaj dio imovine čija se tržišna vrijednost kontinuirano mijenja. Povijesni trošak imovinske pozicije jest novac ili novčani ekvivalent plaćen za stjecanje imovine ili dane fer vrijednosti naknade za stjecanje imovine na datum stjecanja. Povijesni trošak u slučaju stjecanja imovine trošak je stjecanja. Tekući trošak jest iznos novca ili novčanih ekvivalenata koji bi se trebao platiti kada bi se sada steklo isto ili ekvivalentno sredstvo. Tekući trošak zaliha, opreme i uređaja jednak je njihovu trošku zamjene.<sup>32</sup>



**Slika 5.10.** Korištena troškovna baza

*Izvor: Empirijsko istraživanje*

Kao što je istaknuto na početku rada, tele operatori imaju velike udjele indirektnih troškova u ukupnim troškovima i upravo je zato od velike važnosti naći učinkovitu metodu raspodjele tih troškova (Slika 5.11.). Većina operatora ima između 40% i 60% troškova indirektnih, što nije iznenađujuće s obzirom na to da je za telekomunikacijski sektor karakteristično do čak 80% indirektnih troškova.

<sup>31</sup> Gulin, D.: „Računovodstveni aspekti vrednovanja portfelja mirovinskih fondova“, Ekonomski fakultet, Zagreb, 18.12.2001., UDK330.322.368.914

<sup>32</sup> Gulin, D.: „Računovodstveni aspekti vrednovanja portfelja mirovinskih fondova“, Ekonomski fakultet, Zagreb, 18.12.2001., UDK330.322.368.914





**Slika 5.11.** Razredi kretanje udjela indirektnih troškova

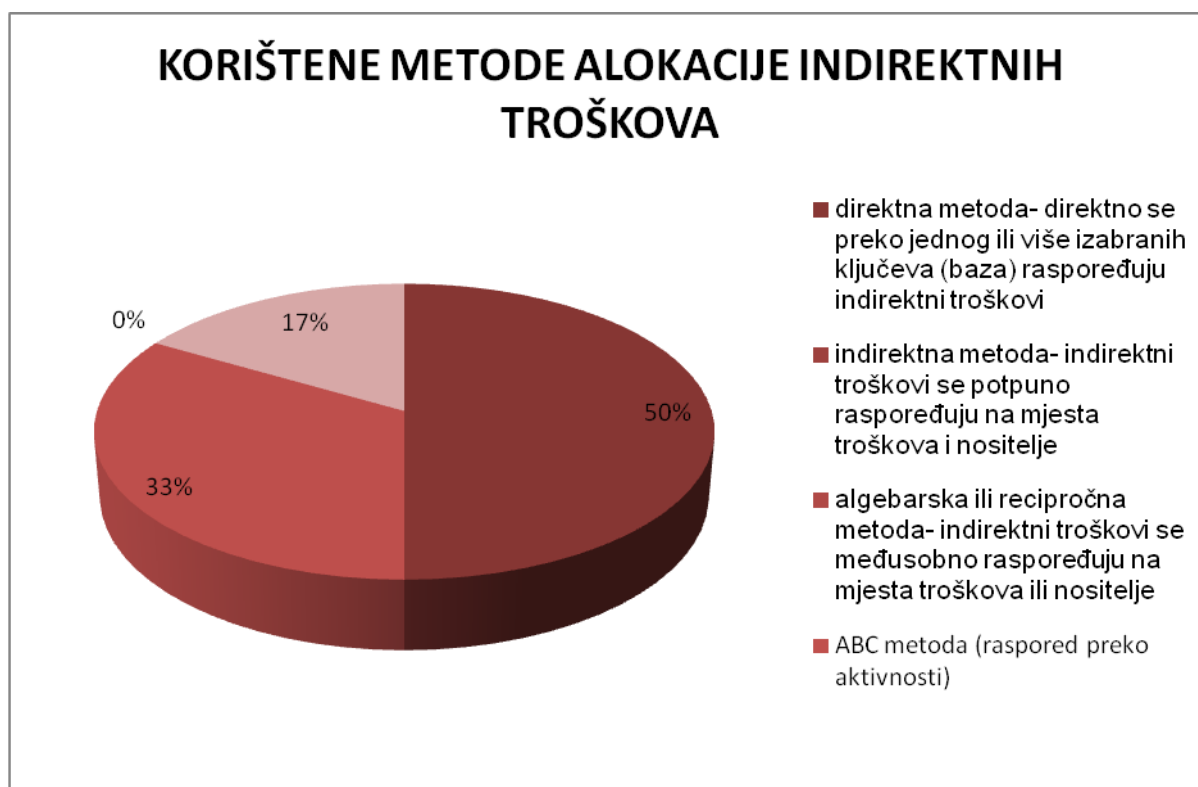
*Izvor: Empirijsko istraživanje*

Pet od šest operatora provodi raspodjelu indirektnih troškova na nositelje pri čemu jedan koristi ABC metodu za računovodstveno praćenje troškova i CVR metodu unutar LRIC metodologije pri sastavljanju financijskih izvještaja, jedan koristi samo ABC metodu dok tri operatora koriste direktnu metodu (Slika 5.12. i 5.13.).



**Slika 5.12.** Provođenje raspodjele indirektnih troškova na nositelje

*Izvor: Empirijsko istraživanje*



**Slika 5.13.** Korištene metode raspodjele indirektnih troškova

*Izvor: Empirijsko istraživanje*

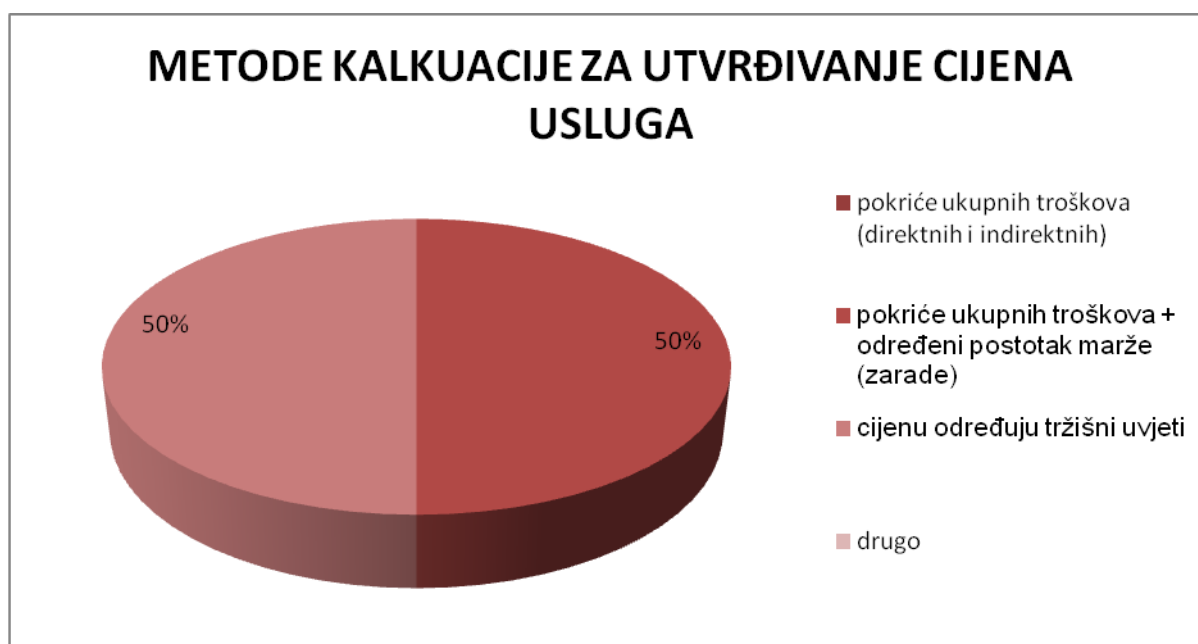
Na pitanje „Koju metodu kalkulacije koristite za utvrđivanje cijena usluga?“ tri operatora su odgovorila da koriste metodu pokrivaća ukupnih troškova + određeni postotak marže (zarade), a tri druga su odgovorila da cijenu određuju tržišni uvjeti (Slika 5.14.).

Ne čudi činjenica da je pola operatora odgovorilo da cijenu određuju tržišni uvjeti s obzirom na to da na brze tehnološke promjene, veliku konkurenciju na tržištu te kontinuirano mijenjanje uvjeta na tržištu. Svim poduzećima, pa tako i operatorima, je u cilju zaraditi i biti konkurentni, a praćenjem tržišnih uvjeta i cijena konkurenata upravo to i postižu.

Kritično niska tržišna cijena kod koje su prihodi upravo jednaki varijabilnim troškovima (AC) (ili, drugim riječima, kad su gubici upravo jednaki fiksnim troškovima) naziva se točka zatvaranja. Dok su cijene iznad točke zatvaranja, poduzeće će nastaviti s proizvodnjom trgom svoje krivulje graničnih troškova (MC) zbog toga što bi, iako time izgubilo novac, više novca izgubilo prestankom proizvodnje. Kad su cijene pak ispod točke zatvaranja poduzeća, ono neće uopće proizvoditi zato što prestankom rada gubi samo svoje fiksne troškove. Točka zatvaranja je tamo gdje prihodi upravo pokrivaju varijabilne troškove ili gdje su gubici jednaki fiksnim troškovima. Kad cijena padne ispod prosječnih varijabilnih troškova, poduzeće će maksimizirati dobit (minimizirati gubitke) tako da prestane s proizvodnjom.<sup>33</sup> Slika 5.15. prikazuje točku zatvaranja i točku nulte dobiti odnosno točku

<sup>33</sup> Samuelson, P., A., Nordhaus, D., W.: „Ekonomija“, MATE d.o.o. Zagreb, 2005.

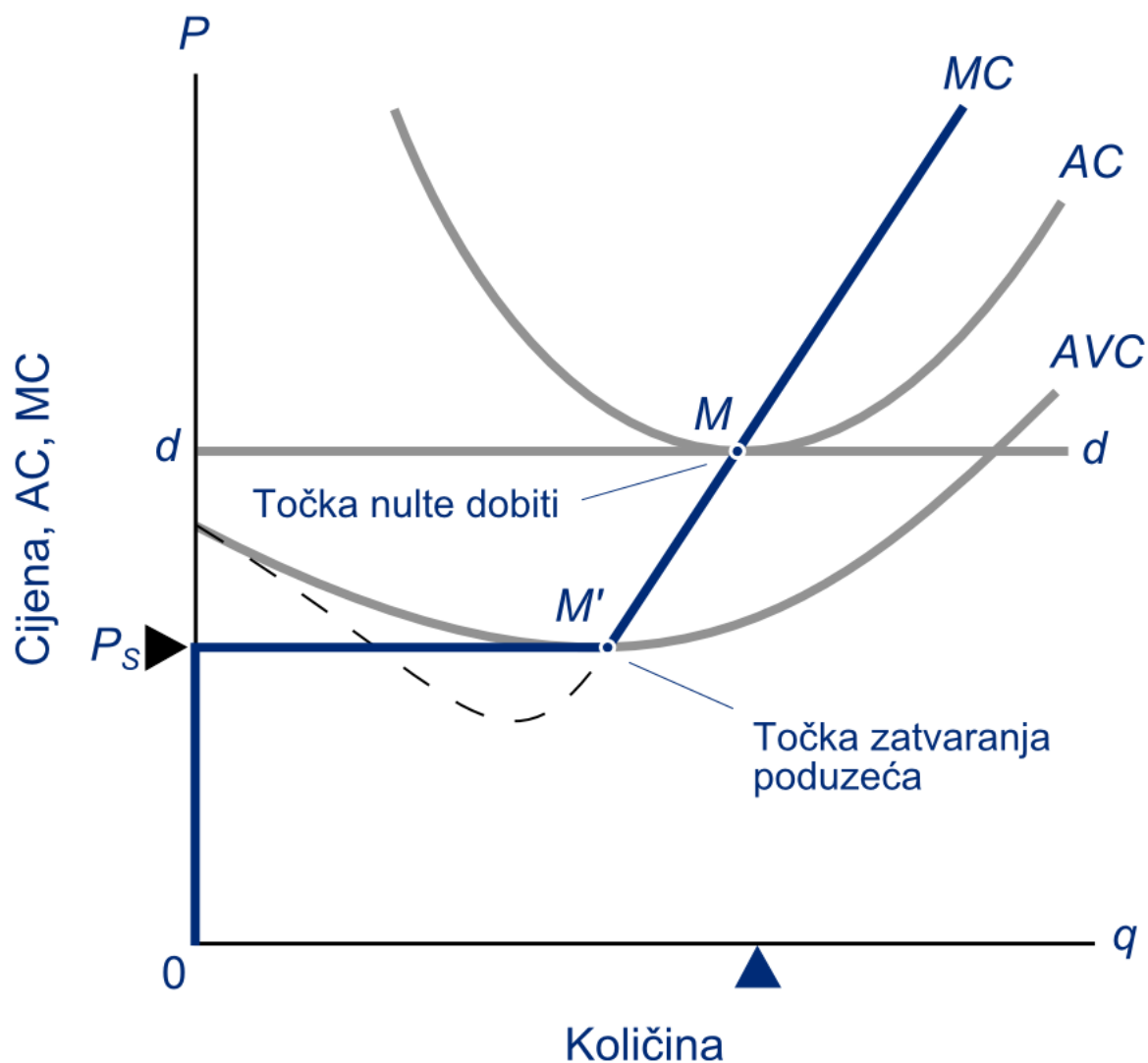
pokrića za neko poduzeće. Točka nulte dobiti odnosno pokrića (M) je tamo gdje je cijena izjednačena s AC dok je razina proizvodnje kod koje dolazi do zatvaranja poduzeća (M') tamo gdje je cijena izjednačena sa prosječnim varijabilnim troškovima (AVC). U točki zatvaranja poduzeća, M', je cijena jednaka graničnim troškovima (MC) i prosječnim varijabilnim troškovima (AVC). U točki M, točki pokrića troškova, je cijena (P) jednaka graničnim troškovima (MC) i prosječnim troškovima (AC) te pravac ponude siječe krivulju MC i dodiruje krivulju AC. Kako bi se uz pokriće troškova ostvarila dobit, potrebno je na tu cijenu dodati određeni postotak marže koja se u ovom slučaju zove kontribucijska marža. Ona označava razliku između prihoda i varijabilnih troškova koja sadrži dio za pokriće fiksnih troškova i dobit.<sup>34</sup>



**Slika 5.14.** Metode kalkulacije za utvrđivanje cijena usluga

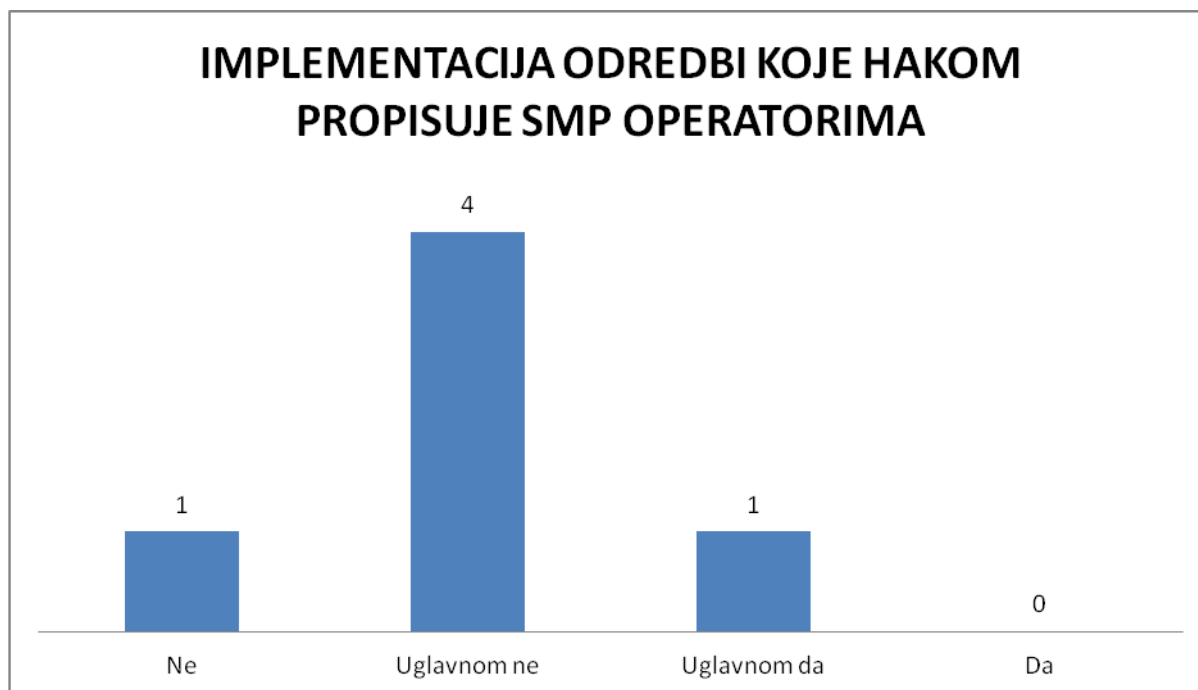
*Izvor: Empirijsko istraživanje*

<sup>34</sup> Kravaica, V.,A.: „Analiza odnosa“, s Interneta, [http://www.veleri.hr/files/datoteke/nastavni\\_materijali/k\\_poduzetnistvo\\_s1/11 - CVP analiza.pdf](http://www.veleri.hr/files/datoteke/nastavni_materijali/k_poduzetnistvo_s1/11_-_CVP_analiza.pdf), 03.02.2014.



**Slika 5.15.** Točka pokrića ukupnih troškova

Na pitanje „Prema Vašem mišljenju, je li postojeći računovodstveni informacijski sustav Vašeg poduzeća usmjeren pretežno na zadovoljavanje odredbi (u smislu izvještavanja i kalkulacije troškova) koje propisuje HAKOM za operatore sa značajnom tržišnom snagom, neovisno o tome da li Vaše poduzeće pripada toj kategoriji ili ne?“ samo je jedan operator odgovorio potvrdno (Slika 5.16.). Odgovori su se mogli pretpostaviti, obzirom da samo jedan operator ima obavezu implementacije HAKOM-ovih odredbi u svoj računovodstveni informacijski sustav. Dobivene informacije na taj način, ispitani operator koristi za donošenje poslovnih odluka.



**Slika 5.16.** Implementacija odredbi koje HAKOM propisuje SMP operatorima

*Izvor: Empirijsko istraživanje*

Kako je istraživanje pokazalo, većina troškova tele operatora su indirektni troškovi, čak do 60% ukupnih troškova u ovom slučaju, koje nije lako raspodijeliti na troškovne objekte te se zato javlja potreba za transparentnim troškovnim upravljanjem. Kako bi troškovno upravljanje dovelo do unaprjeđenja poslovnih proces, bitno je pronaći adekvatnu metodu raspodjele troškova koja će reflektirati vezu između nastalih troškova i ključa za raspodjelu istih na nositelje. Samo dva od šest anketiranih operatora koriste ABC metodu za raspodjelu troškova unutar svojih računovodstvenih informacijskih sustava. Jedan od ta dva koristi ABC metodu unutar FAC metodologije, a drugi koristi ABC metodu unutar VBM metodologije. Osim ABC metode, jedan od ta dva operatora koristi i CVR metodu unutar LRIC metodologije u svrhe sastavljanja financijskih izvještaja zato što ima značajnu tržišnu snagu na telekomunikacijskom tržištu pa je zakonski obavezan koristiti istu. Takvi rezultati ne iznenađuju obzirom da se radi o kompleksnim metodologijama i metodama čije uvođenje u računovodstveni informacijski sustav poduzeća iziskuje velike napore i resurse, a ima smisla u većim kompanijama kojih ima malo na hrvatskom telekomunikacijskom tržištu. Međutim uvođenje sustavne metode raspodjele troškova temelj je učinkovitog upravljanja troškovima i priprema za širenjem poslovanja te implementaciju EU smjernica koja u budućnosti može postati obaveza svih operatora koji žele konkurirati na inozemnim tržištima. Kako su računovodstveni informacijski sustavi operatora koji posluju na hrvatskom tržištu ograničeni, isti bi ih trebali početi restrukturirati jer bi na taj način stvorili dobre temelje za učinkovitim upravljanjem troškova, implementaciju EU smjernica te budućim konkuriranjem na inozemnim tržištima.

### 7.3. Zaključak

Glavno obilježje telekomunikacijskog sektora je dinamično okruženje s neprekidnim tehnološkim promjenama koje uzrokuju promjene u strukturi troškova. Osim tehnoloških inovacija i promjena, automatizacija u poslovnom procesu, digitalizacija, mobilnost podataka, povećanje broja prodajnih usluga te sve zahtjevniji korisnici uzrokovali su povećanje troškova u smislu proizvodnog razvoja, prodaje, poslovne kontrole itd. Većina troškova u telekomunikacijskim kompanijama su indirektni troškovi, čak do 80% ukupnih troškova, koje je teško raspodijeliti na troškovne objekte što uzrokuje potrebu za transparentnim troškovnim upravljanjem.

Temelj uspješnog upravljanja troškovima je jasno definiran sustav upravljačkog računovodstva i odabir najrelevantnijeg instrumenta za upravljanje i obračun troškova, zbog odabira onih usluga koje su profitabilne. Telekomunikacijske kompanije nude mnogobrojne usluge i proizvode koje za posljedicu imaju čitav niz različitih troškova. Kako bi se izračunao jedinični trošak svake te usluge odnosno proizvoda, potrebno je definirati sve prethodno nastale troškove.

U telekomunikacijskoj industriji najčešće se koriste dva instrumenta za upravljanje troškovima odnosno dvije računovodstvene metodologije raspodjele troškova, a to su: metoda potpuno raspodijeljenih troškova (engl. *Fully Alocated Costs*, FAC) i metoda dugoročnih inkrementalnih troškova (engl. *Long Run Incremental Costs*, LRIC). Prema naputcima EU, HAKOM zahtjeva od operatora, sa značajnom tržišnom snagom, pripremu i objavu Regulatornih financijskih izvještaja na temelju računovodstvene metodologije LRIC i metodologije FAC za potrebe računovodstvenog odvajanja.

FAC računovodstvena metodologija raspoređuje sve relevantne nastale troškove, prihode, imovinu i obveze operatora na pripadajuće usluge, uz primjenu načela uzročnosti pomoću ABC metode (engl. *Activity Based Costing System*, ABC). ABC metoda je računovodstveni pristup troškovnom upravljanju koji dozvoljava uspostavu uzročno-posljedičnih odnosa između troškova i usluga ili proizvoda te fokusira pažnju na indirektno troškove.

LRIC predstavlja metodologiju prema kojoj se troškovi na kapitalno intenzivnom tržištu elektroničkih komunikacija, koje na veleprodajnoj razini karakteriziraju značajni troškovi ulaganja i dugi vijek trajanja imovine, mogu analizirati i koristiti za određivanje cijena na troškovno orijentiran način. Omogućava troškovno modeliranje telekomunikacijskih mreža koje se bazira na troškovnoj uzročnosti i mrežnoj iskorištenosti svake omogućene usluge te kao cjenovna politika sprječava pretjerane profite operatora na tržištu.

## 7.4. Literatura

- [1] Direktiva 2002/19/EC Europskog Parlamenta i Vijeća 7. ožujka 2002 na temu pristupa, interkonekcije i elektroničkih komunikacijskih mreža i povezanih usluga (Pristupna Direktiva), s Interneta, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0019:EN:HTML>; 20.02.2013.
- [2] Direktiva 2002/21/EC Europskog Parlamenta i Vijeća 7. ožujka 2002. na temu zajedničkog regulatornog okvira elektroničkih komunikacijskih mreža i usluga (Okvirna Direktiva), s Interneta, <http://eur-lex.europa.eu/Notice.do?mode=dbl&lang=hr&ihmlang=hr&lng1=hr,hr&lng2=bg,cs,da,de,el,en,es,et,fi,fr,hr,hu,it,lt,lv,mt,nl,pl,pt,ro,sk,sl,sv,&val=737602:cs>, 20.02.2013.
- [3] Dražić Lutitsky, I., Broz Tominac, S., Ivić, M. (2011): „Activity based system in telecommunications industry“, 19th International Conference on Software Telecommunications and Computer Networks, Split-Hvar-Dubrovnik, 15.-17. rujan 2011, ISBN 978-953-290-027-9.
- [4] Dražić Lutitsky, I., Ivić, M. (2013): „Valuation of long-term tangible asset under LRIC methodology“, 12th International Conference on Telecommunications, Zagreb, 26.-28. lipnja 2013, ISBN 958-953184-176-4.
- [5] Dunković: „Strateško menadžersko računovodstvo“, s Interneta, [http://bib.irb.hr/datoteka/443463.Skripta\\_RRiF\\_SMR\\_s\\_vjezbama\\_2011.pdf](http://bib.irb.hr/datoteka/443463.Skripta_RRiF_SMR_s_vjezbama_2011.pdf), 08.01.2014.
- [6] Gulin, D.: „Raspoređivanje općih troškova proizvodnje na mjesta i nositelje troškova“, Računovodstvo i financije br. 8/1998.
- [7] Gulin, Danimir: „Raspoređivanje općih troškova proizvodnje (OTP) sporednih i pomoćnih mjesta troškova na glavna mjesta troškova i na nositelje troškova“, s Interneta, <http://web.efzg.hr/dok/RAC/OTP%20raspored.pdf>, 29.01.2013.
- [8] Gulin: „Kriteriji provođenja i postupci konsolidacije financijskih izvještaja“, s Interneta, <http://web.efzg.hr/dok/RAC/Konsolidacija.pdf>; 26.01.2012.
- [9] Hrvatska agencija za poštu i telekomunikacije: „Računovodstveno odvajanje i troškovno računovodstvo“, konzultacijski dokument, Zagreb, kolovoz 2008, s Interneta, [http://www.hakom.hr/userdocsimages/javnarasprava/Microsoft%20Word%20-%20Racunovodstveno%20odvajanje%20i%20troskovno%20racunovodstvo\\_Final%20\\_2\\_.pdf](http://www.hakom.hr/userdocsimages/javnarasprava/Microsoft%20Word%20-%20Racunovodstveno%20odvajanje%20i%20troskovno%20racunovodstvo_Final%20_2_.pdf); 20.02.2013.
- [10] Kravaica, V.,A.: „Analiza odnosa“, s Interneta, [http://www.veleri.hr/files/datoteke/nastavni\\_materijali/k\\_poduzetnistvo\\_s1/11\\_-\\_CVP\\_analiza.pdf](http://www.veleri.hr/files/datoteke/nastavni_materijali/k_poduzetnistvo_s1/11_-_CVP_analiza.pdf), 03.02.2014.

- [11] Lutilsky, D., I., Gulin, D., Sačer, M., I., Tadijančević, S., Tušek, B., Vašiček, V., Žager, K., Žager, L.: “Računovodstvo”, Hrvatska zajednica računovođa i financijskih djelatnika, Zagreb, 2010.
- [12] Perčević, H.: „Utjecaj računovodstvenih metoda alokacije troškova proizvodnje na ocjenu profitabilnosti proizvoda“, magistarski rad obranjen 14.10.2005., Ekonomski fakultet Zagreb
- [13] Perčević, Hrvoje: “Troškovi i kriteriji klasifikacije troškova”, s Interneta, <http://web.efzg.hr/dok/RAC/Tro%C5%A1kovi%20i%20kriteriji%20klasifikacije%20tro%C5%A1kova.pdf>, 08.01.2014.
- [14] Samuelson, P., A., Nordhaus, D., W.: „Ekonomija“, MATE d.o.o. Zagreb, 2005.
- [15] Službene novine Europske Unije, Komisijska Preporuka 2005/698/EC 19. rujna 2005 na temu računovodstvenog odvajanja i troškovnog računovodstva pod regulatornim okvirom elektroničkih komunikacija, s Interneta, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:266:0064:0069:EN:PDF;> 20.02.2013.
- [16] The Independent Regulators Group: „ERG COMMON POSITION: Guidelines for implementing the Commission Recommendation C (2005) 3480 on Accounting Separation & Cost Accounting Systems under the regulatory framework for electronic communications“, s Interneta, [http://www.irg.eu/streaming/erg\\_05\\_29\\_erg\\_cp\\_rec\\_as\\_and\\_cas\\_final.pdf?contentId=543322&field=ATTACHED\\_FILE](http://www.irg.eu/streaming/erg_05_29_erg_cp_rec_as_and_cas_final.pdf?contentId=543322&field=ATTACHED_FILE) 25.01.2012.
- [17] Um, P. N., Gille, L., Simon, L. Rudelle, C.: „A Model for Calculating Interconnection Costs in Telecommunications“, The World Bank, 2004., ISBN 0-8213-5671-2
- [18] Žager, K., Tušek, B., Vašiček, V., Žager, L.: “Osnove računovodstva“, Hrvatska zajednica računovođa i financijskih djelatnika, Zagreb, 2007.



## 8. Radionica „The 4rd Workshop on Regulatory Challenges in the Electronic Communications Market“

Radionica je održana u sklopu međunarodne konferencije *The 22nd Conference on Software, Telecommunications and Computer Networks (SoftCOM 2014)* u Hotelu Radisson Blu Resort u Splitu. Riječ je o četvrtoj u nizu specijaliziranih radionica koje se bave problematikom regulacije novih generacija mreža, inicijalno pokrenute kako bi se promovirali rezultati projekta „Pogled u budućnost 2020“ koji se odvija pod vodstvom Hrvatske regulatorne agencije za mrežne djelatnosti (HAKOM). Od prve tri radionice dvije su također održane u sklopu međunarodne konferencije *Software, Telecommunications and Computer Networks – SoftCOM*, i to 2011. (Hvar) i 2012. (Split) godine. Treća radionica je održana u sklopu međunarodne konferencije *12th International Conference on Telecommunications – ConTEL 2013* u Zagrebu.

Projekt „Pogled u budućnost 2020“ interdisciplinarni je projekt koji uključuje znanstvenike s triju hrvatskih sveučilišta: Sveučilišta u Zagrebu, Sveučilišta u Splitu i Sveučilišta J.J. Strossmayera u Osijeku, kao i predstavnike vodećih telekomunikacijskih kompanija i mrežnih operatora u Hrvatskoj. Područje istraživanja su telekomunikacijski sustavi i elektroničko tržište, s naglaskom na regulacijski aspekt i probleme koji se tu mogu pojaviti. Cilj projekta je stoga razviti proaktivno regulatorno okružje u kojem će se potencijalni problemi moći predvidjeti i što prije ukloniti kako bi se minimizirao njihov negativan utjecaj na razvoj telekomunikacijskog tržišta u Republici Hrvatskoj.

### 8.1. Popis radova

- Vedran Mikac, Željko Ilić, Tomaž Beriša, Alen Bažant, Mladen Kos, Goran Jurin, Velimir Švedek: *Capacity analysis of RT-based VDSL2 copper access networks*
- Višnja Križanović, Drago Žagar, Snježana Rimac-Drlje, Tomislav Švedek: *Business Models and Cost Optimization of Wireless Rural Broadband Access Implementation*
- Mladen Sikirica, Danko Čurepić: *Broadband mapping - Croatian experience*
- Pavle Skočir, Damjan Katušić, Ivan Novotni, Iva Bojić, Gordan Ježić: *Data Rate Fluctuations from User Perspective in 4G Mobile Networks*
- Ignac Lovrek, Antun Carić, Dražen Lučić: *Future Network and Future Internet: A Survey of Regulatory Perspective*
- Nina Gumzej, Dražen Dragičević: *Cloud computing data protection aspects under Croatian and European Union law*
- Ivana Dražić Lutilsky, Marina Ivić: *Accounting information systems of telecommunication operators in Croatia*

- Emil Dumić, Sonja Grgić, Domagoj Frank: *Simulating DVB-T to DVB-T2 Migration Opportunities in Croatian TV Broadcasting*
- Marin Vuković, Damjan Katušić, Pavle Skočir, Dragan Jevtić, Luka Delonga, Daniela Trutin: *User Privacy Risk Calculator*

## 9. Komunikacijski sustav stroja sa strojem u javnoj pokretnoj mreži

### 9.1. Uvod

Snažan razvoj bežičnih tehnologija posljednjih godina ponudio je veliku rasprostranjenost bežične povezivosti i snizio cijene bežičnih modula. To je u kombinaciji s poticajima koje određene zemlje daju za pojedina područja primjene (smart grid, eZdravstvo), a koja su u fokusu komunikacije stroja sa strojem (engl. *Machine-to-Machine*, M2M), privuklo pažnju interesnih skupina i ulagača [1]. Javne pokretne mreže zasnovane na standardima udruge 3GPP (*The 3rd Generation Partnership Project*) imaju nekoliko obilježja koja ih čine obećavajućim rješenjem za implementaciju komunikacijskog sustava stroja za strojem: jednostavan i brz početak rada (za koji na raspolaganju treba imati pretplatnički identifikacijski modul (engl. *Subscriber Identity Module*, SIM)), vrlo dobra pokrivenost signalom, podrška za komunikaciju protokolom IP (*Internet Protocol*), podrška pokretljivosti i izvrsne karakteristike u pogledu mrežne propusnosti i kašnjenja. Razvoj standarda udruge 3GPP vezan uz komunikaciju stroja sa strojem u javnoj pokretnoj mreži detaljnije je opisan u HAKOM izvještaju [2] iz 3. kvartala 2012. godine. Rad [3] objavljen u sklopu radionice „The 3rd Workshop on Regulatory Challenges in the Electronic Communications“ na konferenciji ConTEL 2013 daje osvrt na arhitekturu i moguće primjene takvih sustava, prikazuje aktualno stanje na tržištu i navodi regulacijske napore provedene u Republici Hrvatskoj kako bi se M2M komunikacija što lakše uvela u javne pokretne mreže. Istraživanje izneseno u [4] analizira integraciju M2M tehnologija u novu generaciju pokretnih sustava, dugoročnu evoluciju mreže (engl. *Long Term Evolution*, LTE).

Sljedeće poglavlje iznosi specifična obilježja M2M komunikacije koja zahtijevaju prilagodbu postojećih javnih pokretnih mreža kako bi bolje funkcionirala. Predložena su dva osnovna scenarija M2M komunikacije, kao i rješenja za njihovo uvođenje u zadnju implemetiranu generaciju javnih pokretnih mreža, LTE. Treće poglavlje govori o potencijalnim promjenama na tržištu M2M modula koje predviđaju porast u korištenju upravo LTE mreža, dok četvrto poglavlje daje pregled stanja na tržištu M2M platformi. Peto poglavlje iznosi izazove s kojima se proizvođači opreme, mrežni operatori i regulatori moraju ozbiljnije pozabaviti sada i u bližoj budućnosti žele li zadržati sadašnju snažnu stopu rasta M2M tržišta.

### 9.2. Specifičnosti M2M komunikacije u javnoj pokretnoj mreži

Trenutne su tehnologije javne pokretne mreže dizajnirane i prilagođene ljudskoj komunikaciji: govornim pozivima, slanju SMS/MMS poruka te podatkovnoj komunikaciji, u kojoj korisnici pristupaju poslužiteljima i skidaju (engl. *download*) ili iniciraju strujanje (engl. *stream*) dostupnog sadržaja. Međutim, to istodobno znači da te mrežne tehnologije nisu optimizirane za specifičnu komunikaciju koja se odvija između potencijalno autonomnih i inteligentnih umreženih strojeva. Komunikacija stroja sa strojem podrazumijeva vrlo malo ili nikakvo uplitanje od strane čovjeka. U većini situacija u kojima čovjek sudjeluje, čini to kao

primatelj, a ne inicijator komunikacije [5]. Tablica 1.1. prikazuje osnovne razlike između komunikacije između ljudi (H2H) i komunikacije stroja sa strojem (M2M).

**Tablica 1.1.** Razlike između H2H i M2M komunikacije

Tema	H2H	M2M
<b>Gustoća</b>	Penetracija bežičnih uređaja u blagom je porastu. I dalje postoji potencijal za daljnji rast na slabije razvijenim tržištima.	Potencijalan broj umreženih strojeva uvelike nadmašuje ljudske korisnike, što je jedan od razloga za brže uvođenje protokola IPv6. Mogući su problemi s adresiranjem, nedostatkom telefonskih brojeva itd.
<b>Podaci</b>	Glavnina podatkovnog prometa ide u dolaznom smjeru (engl. <i>download</i> ), a odnosi se na razmjenu sadržaja i zahtijeva značajne količine prijenosnog kapaciteta (prijenos datoteka, pregledavanje <i>weba</i> , strujanje video-sadržaja)	Većina usluga tipično zahtijeva male količine prometnog kapaciteta i to u odlaznom smjeru (engl. <i>upload</i> ). Postoje iznimke, npr. usluga video nadzora.
<b>Baterija</b>	Zamjena baterije nije značajan problem; kupi se nova i zamjeni ili nadopuni postojeća.	Od baterija se zahtijeva mogućnost samo-obnavljanja i/ili dugotrajnost (na duže vremenske periode).
<b>Kašnjenje</b>	Ljudski korisnici spremni su tolerirati manja kašnjenja, čak i kada je u pitanju stvarno-vremenska govorna komunikacija.	Neke aplikacije (npr. daljinski nadzor) zahtijevaju stvarno-vremenski pristup; hitne akcije imaju vrlo malu toleranciju kašnjenja.
<b>Sigurnost</b>	Vrlo dobra. U nekim situacijama (npr. krađa uređaja), ljudski korisnici reagiraju instinktivno ili znaju što se događa.	Izrazito veliki problemi. Zahtijevaju se dodatni naponi kako bi se postigla veća sigurnost i robusnost mreže. Trenutno se razmatra uvođenje modula MCIM ( <i>Machine Communication Identity Module</i> ) u okviru UICC-a ( <i>Universal Integrated Circuit Card</i> ) ili okoline povjerenja (engl. <i>Trusted Environment</i> , TRE)
<b>Prihodi</b>	Prosječan prihod po korisniku (engl. <i>Average Revenue Per User</i> , ARPU) je vrlo dobar.	Prosječan prihod po stroju (engl. <i>Average Revenue Per Device</i> , ARPD) znatno je manji od ARPU-a (tipično iznosi oko 10% od ARPU). Održavanje poslovnog modela očekuje se povećanim brojem umreženih strojeva.
<b>Dimenzioniranje</b>	Normalni poslovni slučaj.	Veliki broj krajnjih umreženih strojeva koji se povremeno spajaju na mrežu i šalju male količine podataka. Međutim, zbog njihovog velikog broja ne smiju se zanemariti potencijalna mrežna preopterećenja.
<b>Pristup čvorovima</b>	Zadovoljavajući.	Temelji se na modelu <i>push/pull</i> . Zahtijeva nešto duže periode pauze kako bi se smanjila signalizacija.

Jedan od ključnih rezultata standardizacije u okviru 3GPP-a definicija je 14 specifičnih obilježja komunikacije [6] na koje valja obratiti pozornost kada se razmatra optimizacija

javne pokretne mreže zasnovane na 3GPP tehnologijama za komunikaciju stroja sa strojem (Tablica 1.2.).

**Tablica 1.2.** Specifičnosti M2M komunikacije

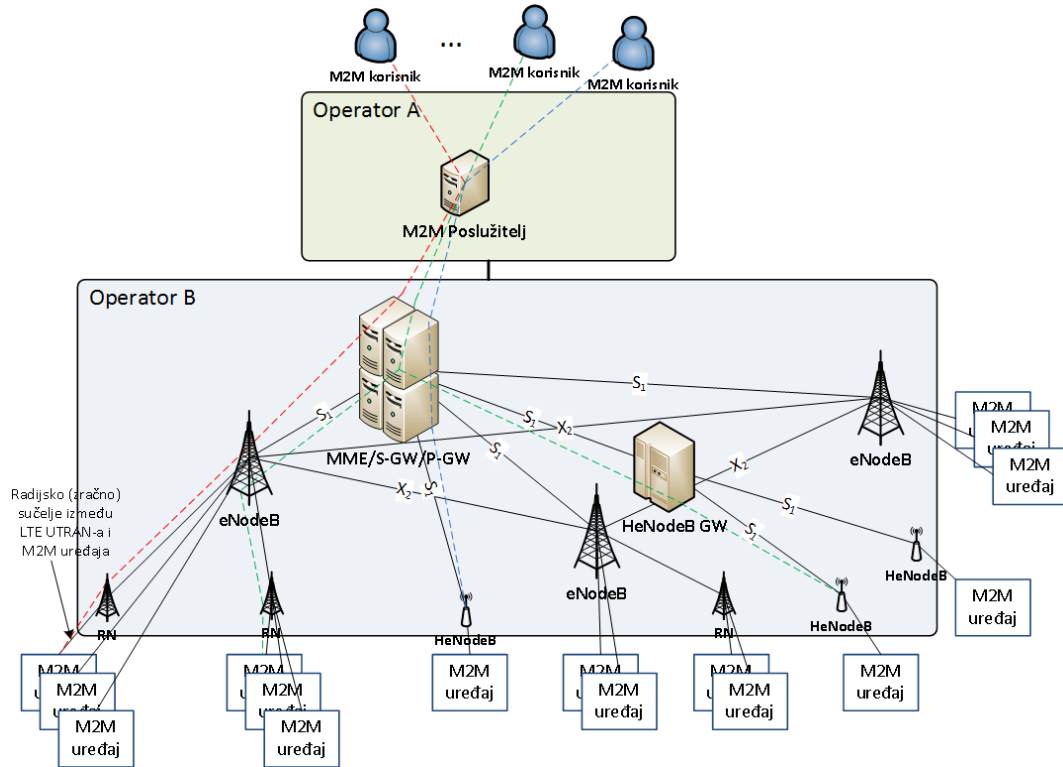
Obilježje	Opis
Slaba pokretljivost (engl. <i>Low Mobility</i> )	Umreženi strojevi tipično su nepokretni, nomadski ili se kreću unutar unaprijed definiranog područja, što omogućuje optimizaciju signalizacije.
Vremenska kontrola (engl. <i>Time Controlled</i> )	Podaci se šalju/primaju samo unutar unaprijed definiranih vremenskih intervala, čime se signalizacija izvan tih vremenskih prozora značajno smanjuje.
Tolerancija na vremensko kašnjenje (engl. <i>Time Tolerant</i> )	Podatkovne aplikacije podržavaju kašnjenja odnosno odgode prilikom slanja podataka.
Podrška za paketske usluge (engl. <i>Packet Switched Only</i> )	Mrežni pristup omogućuje pristup uslugama i dohvaćanje strojeva bez uporabe telefonskog broja (engl. <i>Mobile Station International Subscriber Directory Number, MSISDN</i> ).
Prijenosi malih količina podataka (engl. <i>Small Data Transmissions</i> )	Većina umreženih strojeva šalje/prima male količine podataka.
Optimizacija izvora 1 (engl. <i>Mobile Originated Only</i> )	Mreža treba omogućiti mehanizme za smanjenje kontrolne signalizacije koja se šalje iz umreženog stroja, a koji podržava samo taj vid komunikacije.
Optimizacija izvora 2 (engl. <i>Infrequent Mobile Terminated</i> )	Gotovo identično prošlom obilježju. Razlika je u tome što se odnosi na strojeve koji su uglavnom izvori komunikacije.
Nadgledanje umreženog stroja (engl. <i>MTC Monitoring</i> )	Nije namijenjeno sprečavanju krađe stroja. Omogućuje detekciju neočekivanih događaja ili gubitaka veze, o čemu se obavještava krajnji korisnik i poduzimaju unaprijed pripremljene akcije.
Prioritetne poruke (engl. <i>Priority Alarm Message</i> )	Koriste se u situacijama krađe, uzbune ili hitnih slučajeva.
Sigurna veza (engl. <i>Secure Connection</i> )	Primjenjuje se prilikom ostvarivanja sigurne veze između umreženih strojeva i poslužitelja, čak i kada su strojevi u prelaženju između mreža (engl. <i>roaming</i> ).
Okidač lokacije (engl. <i>Location Specific Trigger</i> )	Mrežni operator sprema informaciju o lokaciji umreženog stroja pomoću koje mu može pristupiti kada se isti nađe u određenom području.
Adresa za slanje podataka (engl. <i>Network Provided Destination for Uplink Data</i> )	Omogućuje slanje podataka na specifičnu odredišnu adresu.
Diskontinuirani prijenos podataka (engl. <i>Infrequent Transmission</i> )	Umreženi strojevi diskontinuirano šalju/primaju podatke. Mrežni resursi koriste se samo kada je to doista potrebno.
Grupna obilježja umreženih strojeva (engl. <i>Group Based MTC Features</i> )	Omogućeno je slanje podataka grupi umreženih strojeva odjednom (engl. <i>broadcast</i> ). Omogućeno je korištenje ujednačenih politika naplate, adresiranja i kvalitete usluge (engl. <i>Quality of Service, QoS</i> ) za grupe umreženih strojeva.

U radu [4] predložena su dva osnovna scenarija M2M komunikacije u okviru LTE mreže: prvi je između M2M uređaja i M2M poslužitelja, dok je drugi između dva M2M uređaja.

### 9.2.1. Scenarij M2M uređaj-M2M poslužitelj

U prvom scenariju, prikazanom na Slici 1.1., M2M korisnik (npr. elektrana kao dio smart-grid mreže, senzor u klima-uređaju itd.) može putem M2M poslužitelja upravljati velikim brojem M2M uređaja. Uslugu M2M poslužitelja pruža mrežni operator. Infrastruktura mreže LTE i pripadajući M2M poslužitelji mogu biti razdvojeni između dva operatora ili spadati u domenu istog operatora, kao što je slučaj na slici. 3GPP također dozvoljava scenarij u kojem su M2M poslužitelji smješteni izvan domene operatora. S obzirom da je LTE heterogena mreža s različitim pristupnim rješenjima, uz klasične makročelije s čvorovima eNodeB mogu postojati i pikoćelije s čvorovima eNodeB, makročelije starijih generacije (2G/3G, na slici označeni samo kao RN (engl. *radio network*)) i femtoćelije s čvorovima tipa HeNodeB. Sučelje između

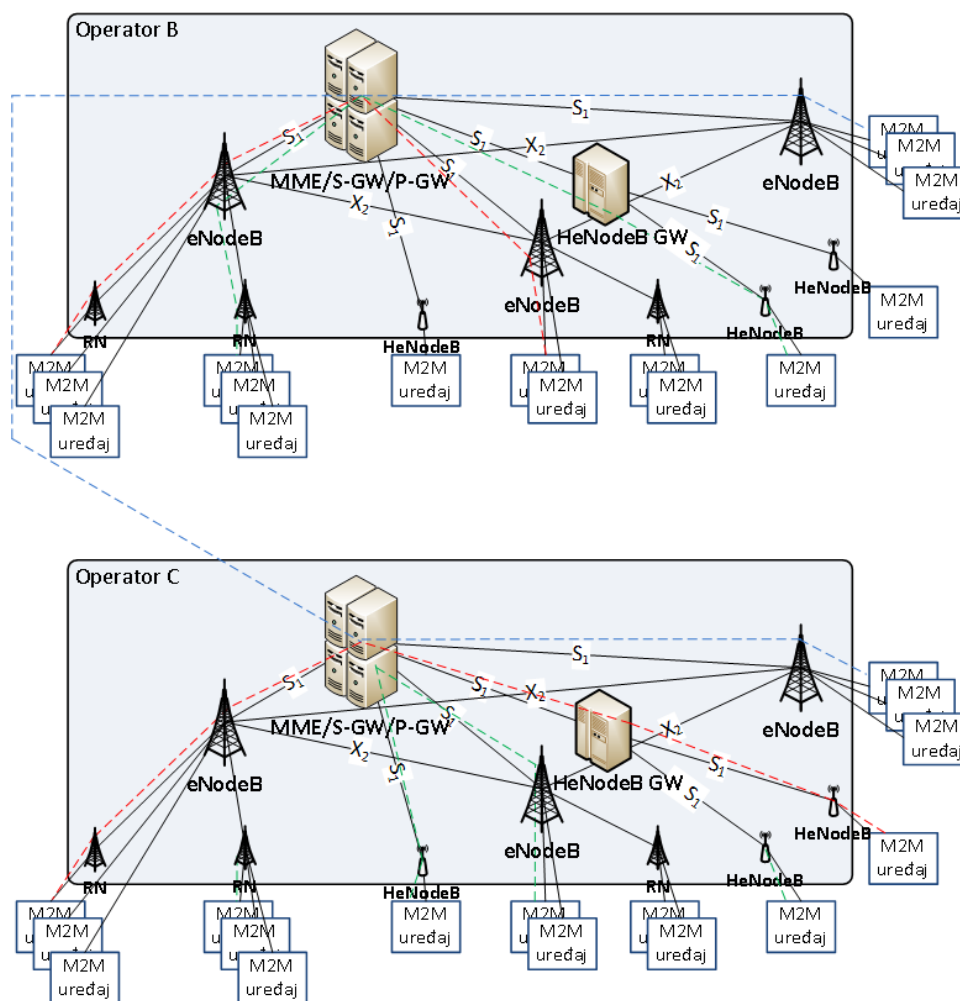
entiteta za upravljanje pokretljivošću (engl. *Mobility Management Entity*, MME) i čvorova tipa eNodeB je  $S_1$ , dok oni međusobno komuniciraju putem sučelja  $X_2$ . Čvorovi HeNodeB i RN također komuniciraju s jezgrenom dijelom mreže LTE putem sučelja  $S_1$ . Prema tome, M2M korisnicima se putem M2M poslužitelja omogućuje upravljanje s većim brojem M2M uređaja spojenih na mrežu LTE. Važno je napomenuti da ovaj scenarij podrazumijeva autorizaciju i autentifikaciju M2M uređaja prije nego li se dozvoli daljnja interakcija s M2M poslužiteljima.



Slika 1.1. Scenarij M2M uređaj-M2M poslužitelj

### 9.2.2. Scenarij M2M uređaj-M2M uređaj

Slika 1.2. prikazuje alternativni scenarij u kojem M2M uređaji komuniciraju međusobno bez posredovanja M2M poslužitelja. Komunikacija se može ostvariti između M2M uređaja koji pripadaju istom ili različitim mrežnim operatorima, no u oba slučaja kao i u prvom scenariju, infrastruktura mreže LTE odgovorna je za povezivanje M2M uređaja i prosljeđivanje paketa između njih.

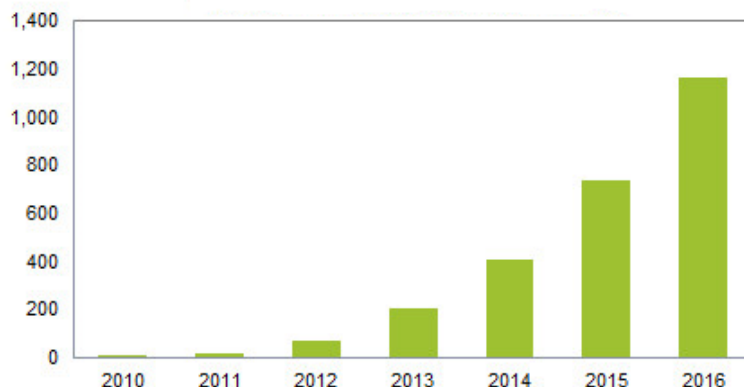


Slika 1.2. Scenarij M2M uređaj-M2M uređaj

### 9.3. Promjene na tržištu M2M modula u javnoj pokretnoj mreži

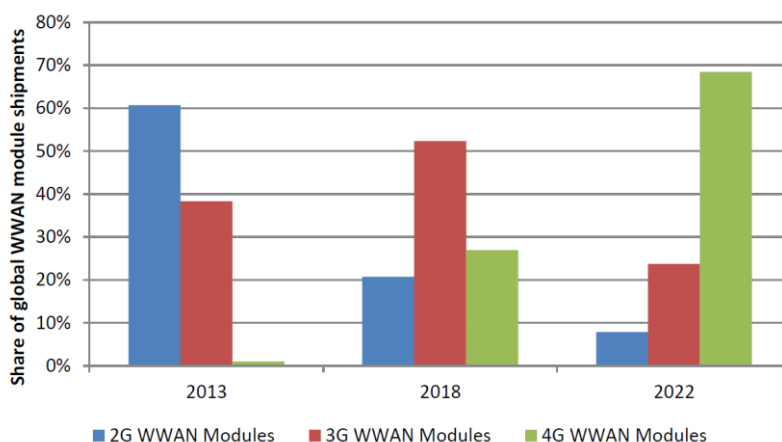
Javne pokretne mreže danas se sastoje od nekoliko suradujućih generacija standarda (GSM/GPRS/UMTS/LTE) koji pružaju uslugu krajnjim korisnicima, i to uglavnom ljudskim korisnicima za čije su ponašanje optimizirani. Pokrivenost mrežnog standarda LTE i broj njegovih pretplatnika zadnjih nekoliko godina raste i po procjenama će nastaviti sve brže rasti (Slika 1.3.), što značajno doprinosi sposobnostima mrežnih operatora za pružanje podatkovnih usluga. Međutim, govorne su usluge i dalje dominantno zasnovane na 2G tehnologijama, odnosno na globalnom sustavu za mobilne komunikacije (engl. *Global System for Mobile Communications*, GSM). Ta činjenica ima vrlo bitan utjecaj na jednu posebno atraktivnu značajku komunikacijskih sustava stroja sa strojem, gubitak pretplatnika (engl. *churn*). Za razliku od pokretnih uređaja namijenjenih ljudskim korisnicima, M2M uređaji bi trebali raditi na istoj mreži sljedećih 10-15 godina ili čak i više. Drugim riječima, vrlo nizak ili nepostojeći odljev M2M uređaja mogao bi natjerati mrežne operatore da i dalje održavaju svoje sadašnje 2G i 3G mreže, pogotovo u slučaju usluga koje koriste malu propusnost, kao što je to slučaj s

čitavim nizom M2M aplikacija (npr. očitavanja sa senzora, praćenje tereta, zdravstvo na daljinu itd.).



**Slika 1.3.** Broj korisnika LTE mreže u svijetu (u milijunima) [izvor: IHS iSupply Research, 2012]

Nova predviđanja iznesena u [7] donose nešto drugačiju priču. Po njima se tržište M2M modula nalazi na prekretnici koja bi mogla iz temelja uzdrmati dosadašnje trendove. Na globalnoj razini, od ukupno 266.5 milijuna M2M konekcija zasnovanih na bežičnim mrežama velikog dometa (engl. *Wireless Wide Area Network, WWAN*), čak 99.5% njih se odnosi na 2G i 3G javne pokretne mreže. Do sada je LTE u kontekstu M2M komunikacije imao vrlo ograničenu primjenu u svega nekoliko aplikacija koje su zahtijevale visoku propusnost. Primjeri su hitne intervencije (engl. *emergency response*), strujanje videa sa sigurnosnih kamera (engl. *security video*) i sustav zabave u automobilima (engl. *automobile entertainment*). Međutim, sadašnje stanje u javnim pokretnim mrežama koje su s jedne strane suočene s povlačenjem 2G mreža, a sve bržim širenjem 4G mreža s druge strane, moglo bi stvoriti savršene uvjete za ubrzano širenje LTE mreža i na komunikacijske sustave stroja sa strojem. Sve veća pokrivenost i sve veći broj pretplatnika donose veća ulaganja u kvalitetu LTE-M2M modula i istodobno snižavaju cijenu njihovog razvoja i proizvodnje [7]. Navedeni trend se već polako uočava na najrazvijenijim tržištima pokretnih mreža, poput SAD-a, Japana, Južne Koreje, Kine i najrazvijenih zemalja Europe, pa se pretpostavlja da će ona biti nosioci promjena koje su navedene na Slici 1.4.



**Slika 1.4.** Predviđeni trend korištenja LTE M2M modula 2013-2022 [izvor: Machina Research, 2013]



Predviđa se da će nadolazeći val novih LTE modula i M2M povezivosti zasnovane na LTE mrežama biti nosioc razvoja i inovacija u području M2M modula te da će prisiliti mnoge sadašnje implementacije M2M sustava na prijelaz s 2G/3G mreža na 4G. Neposredni utjecaj tih nadolazećih promjena prije svega će se osjetiti na prvim tržištima koja obave migraciju i ona će poslužiti kao svojevrsni studijski slučajevi nad kojima će se vršiti procjene isplativosti. Ključni utjecaj ove migracije mogao bi biti na tvrtke koje trenutno raspolažu s velikim M2M implementacijama na 2G pokretnim mrežama ili u narednim godinama planiraju uspostaviti nove, također s velikim brojem M2M uređaja. Migracija će osim na mrežne operatore i pružatelje M2M usluga imati veliki utjecaj i na proizvođače M2M modula. Svi oni će prije svega morati procijeniti troškove migracije te vidjeti isplati li im se s obzirom na specifičnosti pojedinih M2M aplikacija krenuti sada ili možda pričekati još nekoliko godina. Sadašnje 2G pokretne mreže su i dalje dovoljno dobre za većinu mogućih aplikacija, no najavljeno širenje LTE mreža vjerojatno se neće dogoditi bez postupnog gašenja tih „starih“ 2G mreža. S obzirom da je predviđeni životni vijek nekih aplikacija komunikacijskih sustava stroja sa strojem dosta duži od 2-3 godine, izbor mrežne tehnologije M2M modula biti će ključna odluka s dalekosežnim posljedicama.

#### **9.4. Evolucija M2M platformi**

Interoperabilnost M2M platformi za potporu povezivanju (engl. *connectivity support platform*), tj. podrška platforme za spajanje različitih uređaja na različite mrežne tehnologije jedno je od aktualnih pitanja s kojima se regulatori mrežnih djelatnosti tek trebaju ozbiljnije uhvatiti u koštac. Platforme za potporu povezivanju imaju dvojaku ulogu: pružaju usluge *provisioninga* i upravljanja uređajima mrežnim operatorima čija se mrežna infrastruktura koristi i tvrtkama za pružanje M2M usluga [8]. One su vrlo važan element poslovnih strategija mrežnih operatora javne pokretne mreže (engl. *mobile network operator*, MNO). MNO-i se mogu odlučiti na jednu od dvije strategije: prva je razvoj vlastite platforme za potporu povezivanja M2M uređaja, a druga je kupovina gotovog rješenja ili sklapanje strateškog partnerstva sa specijaliziranim pružateljem usluge M2M platforme povezivanja. Odluče li se za prvu strategiju, mrežni operatori mogu ostvariti veću dobit po svakoj pojedinačnoj konekciji M2M uređaja, ali uz preuzimanje veće odgovornosti za održavanje usluge i za krajnje korisnike usluge. Druga strategija sa sobom donosi snižavanje ukupne cijene pružanja M2M usluga, ali i podjelu kontrole i prihoda nad krajnjim korisnicima [8]. Svaki novi uređaj koji se želi spojiti na javnu pokretnu mrežu, a usput i na M2M platformu za potporu povezivanju, prije toga mora biti certificiran. Zemlje članice Europske Unije propisuju slijedeće zahtjeve prilikom certificiranja novih M2M modula: direktive RoHS (*Restriction of Hazardous Substances* [9]), WEE (*Waste Electrical and Electronic Equipment* [10]) i R&TTE (*Radio Equipment and Telecommunications Terminal Equipment and the Mutual Recognition of their Conformity* [11]) koje nastoje smanjiti rizike od širenja opasnih supstanci, zatim reguliraju GSM radijski spektar, brinu o elektromagnetskoj kompatibilnosti modula i niskonaponske opreme [12]. Neki od mrežnih operatora dodatno propisuju i provode svoje vlastite postupke certificiranja. Krajnji cilj je spriječiti sigurnosnu štetu koju novi i do tada neprovjereni M2M uređaji mogu prouzročiti na mrežama na koje se spajaju. Mrežni operatori

su trajanje navedenog procesa certificiranja uspjeli smanjiti s inicijalnih nekoliko mjeseci na svega nekoliko tjedana, i time značajno povećali broj uređaja kojima je dozvoljeno povezivanje koristeći njihovu jezgrenu mrežnu infrastrukturu. Međutim, navedeni je proces do nedavno bio dodatno opterećen ograničenom interoperabilnošću M2M platformi za potporu povezivanju. Otvoreno rješenje M2M platforme u smislu da nije striktno vezano uz samo jednog mrežnog operatora dodatno bi rasteretilo i olakšalo proces certificiranja novih M2M uređaja. Takav bi pristup omogućio puno lakši prelazak uređaja koji je odobren za korištenje na jednoj mreži na mrežu drugog mrežnog operatora, jer se proces certificiranja ne bi trebao ponovno provoditi.

Izvešće [13] predviđa značajne promjene u hijerarhiji M2M platformi, s golemim posljedicama na mnoge sudionike na aktualnim tržištima komunikacijskih sustava stroja sa strojem. Tijekom zadnjeg desetljeća nastao je čitav raspon platformi koje pomažu pri razvoju novih M2M aplikacija. Sve do nedavno, M2M platforme su bile specijalizirane za pojedinačne „vertikalne“ aplikacije te nisu podržavale interoperabilnost razvijenih rješenja. Tek nedavno postaju „otvorena okruženja“ koja razvojnim programerima daju veću slobodu i fleksibilnost pri razvoju aplikacija te pojednostavljaju čitav proces omogućivši kombiniranje više različitih područja primjene. Taj novi tip M2M platformi obično se klasificira kao aplikacijska M2M platforma (engl. *application platform*). Glavni igrači na tom novom rastućem tržištu su Xively [14] (koji su usredotočeni na razvoj usluga s dodanom vrijednošću), ThingWorx [15] (koji nastoje pružiti podršku i za vertikalne aplikacije koje i dalje čine potporanj M2M sustava) i Bosch Software Innovations [16] (koji potencijalnim klijentima donose sposobnost integracije sustava). Spomenute platforme jasno pokazuju da je fokus na horizontalnim komponentama koje omogućuju fleksibilan razvoj usluga za područje komunikacijskih sustava stroja sa strojem i tzv. Interneta stvari (engl. *Internet of Things*, IoT), uz dodatak upravljačkog okruženja. Međutim, aplikacijske M2M platforme unatoč svim svojim prednostima ne smiju se smatrati univerzalnim rješenjem koje će riješiti sve probleme razvoja M2M aplikacija. One bi trebale poslužiti kao sučelja između različitih vertikalnih modula na jednoj strani, i raznih M2M uređaja i komunikacijskih modula na drugoj strani. To samo po sebi nije dovoljno, tako da će svaki potencijalni pružatelj M2M/IoT aplikacijske platforme morati značajno proširiti tu osnovnu funkcionalnost kako bi privukao razvojne programere na korištenje njihove platforme. U svakom slučaju, nove aplikacijske platforme remete odnose koji su uspostavljeni između starijih tipova M2M platformi, a utjecaj na njih će biti raznolik. Aplikacijske potporne platforme (engl. *application support platforms*) će najvjerojatnije biti najteže pogođene. Najbolja strategija će im biti uspostavljanje suradnje s nadolazećim aplikacijskim platformama poput ThingWorxa i iskorištavanje njihovih mogućnosti. Platforme za potporu povezivanju (engl. *connectivity support platform*) i omogućavanje usluga (engl. *service enablement platform*) će se kako bi zadržale konkurentnost ponovno morati fokusirati na usko područje svoje definicije, potpori povezivanju M2M uređaja i omogućavanju usluga. Pružatelji usluga (engl. *solution providers*) bi trebali iskoristiti potencijal M2M aplikacijskih platformi za povećanje prihoda u drugim područjima svoje djelatnosti. Integratori sustava (engl. *systems integrators*) će najvjerojatnije pružati uslugu aplikacijskih M2M platformi besplatno, dodatno narušavajući postojeće odnose na tržištu. Platforme za upravljanje uređajima (engl. *device management platforms*) neće

pretrpjeti značajnije gubitke tako da uspon aplikacijskih platformi neće imati preveliki utjecaj na njih. Međutim, sama pojava ove nove platformske paradigme neće dugo opstati na ovom vrlo konkurentnom tržištu neće li se uspjeti kontinuirano prilagođavati promjenama te nuditi nova i naprednija rješenja za razvoj M2M aplikacija, a jedna od glavnih stavki koju će na neki način morati podržati su semantičke mreže stvari (engl. *Semantic Web of Things*).

### **9.5. Aktualni izazovi u području M2M regulacije**

Regulacija M2M tržišta je s obzirom na dinamiku promjena na tom tržištu konstantno suočena s novim „problemima“ koje treba rješavati. Ostatak poglavlja navodi nekoliko aktualnih problema koje treba ponajprije promatrati iz perspektive regulatora i probati riješiti. Uvijek se postavlja pitanje koliko je regulacije dobro u konkretnoj situaciji i kakav će njen utjecaj biti na daljnji razvoj tržišta.

Trajno prelaženje između mreža (engl. *permanent roaming*): Odnosi se na mogućnost pružanja M2M usluga na globalnoj razini, što je jedan od ključnih preduvjeta za usluge iz sektora prijevoza tereta, automobilskih sustava i potrošačke elektronike. Zabrani li se na regulatornoj razini takva mogućnost *de facto* slobodnog prijelaza između niza javnih pokretnih mreža na praktički globalnoj razini, posljedice bi se za navedene sektore usluga mogle biti dugotrajna stagnacija i pad daljnjih ulaganja. Uz priču o trajnom prelaženju uvijek je jednim dijelom vezano i (među)nacionalno prelaženje (engl. *national roaming*). Trenutni stav regulatora oko trajnog prelaženja je dosta nejasan: oko 80% analiziranih regulatora u izvješću [17] nema nikakvih eksplicitnih pravila. Predviđanja su da bi se regulacija po tom pitanju, naročito u Europi, mogla postrožiti. Takav rasplet događanja, ako se ostvari, će imati značajne posljedice na usluge koje se oslanjaju na uslugu prelaženja bilo zbog potrebe (mrežni operator svojim signalom pokriva ograničeno geografsko područje) bilo zbog izbora (zbog činjenice da SIM kartice mogu iskoristiti pogodnosti nacionalnog prelaženja).

Numeriranje (engl. *numbering*): Regulatori mogu definirati poseban raspon brojeva namijenjen korištenju isključivo za pružanje M2M usluga. Po trenutnim procjenama u [17], otprilike trećina promatranih regulatora (većina je iz Europe) je uvela posebne planove numeriranja namijenjene komunikacijskim uslugama stroja sa strojem. Trenutno ne postoje jasni pokazatelji donosi li takav potez kompetitivnu prednost za brži razvoj M2M tržišta.

Suverenitet nad podacima (engl. *data sovereignty*): Problem suvereniteta nad podacima tiče se načina na koji se upravlja podacima. Različite zemlje se poprilično razlikuju po pitanju smiju li i na koji način neki podaci uopće napustiti teritorij pojedine zemlje. Težina obveza pri rukovanju s podacima koje će se definirati (ako već nisu definirane) u pojedinim zemljama će itekako imati utjecaj na M2M usluge. Također, trenutno mnogi regulatori ne razlikuju jasno sadržaj podataka koji se izmjenjuje između korisnika od komunikacijskih podataka sakupljenih pružanjem pojedine usluge na mrežnoj infrastrukturi. Europska Unija u ovom slučaju ima dosta razrađenu regulativu (EU e-Privacy directive [18]) koja se ne tiče samo priče oko Googlea i prava pojedinca da „bude zaboravljen“, već itekako utječe na koji način

M2M/IoT usluge mogu baratiti s korisničkim podacima, gdje ih smiju spremati i kako dugo zadržati.

Licenciranje spektra (engl. *spectrum licensing*): Trenutno ne postoji posebno definirani dio spektra namijenjen isključivo M2M uslugama, za razliku od primjerice ranije definiranog plana numeriranja. Regulatori u Europi i Sjevernoj Americi trenutno razmatraju potencijalna rješenja, a među kandidatima su tzv. „white space“ spektar koji je telekomunikacijski govoreći frekvencijski pojas koji je dodijeljen za neku namjenu, ali nije u uporabi, te spektar ultra-visokih frekvencija (engl. *Ultra High Frequency*, UHF). Postoje i neke ideje oko korištenja alternativnih tehnologija poput pokrivanja širokog područja niskom snagom (engl. *Low Power Wide Area*, LPWA), no u ovom slučaju postoji dosta nejasnoća oko licenciranja.

Uz navedene, postoji još čitav niz regulatornih problema koje tek treba riješiti, a koji će itekako imati utjecaj na daljnju dinamiku razvoja M2M tržišta. U njih se ubrajaju pitanje registracije i oporezivanja pretplatnika te korištenje novih tehnologija SIM kartica.

## 9.6. Literatura

- [1] K. Chang, A. Soong, M. Tseng, Z. Xiang: „Global Wireless Machine-to-Machine Standardization“, *IEEE Internet Computing*, vol. 15(2), pp. 64-69, 2011.
- [2] Razvoj M2M tržišta, izvješće „Računarstvo u oblaku, M2M, širokopojasni pristup te ekonomski učinci regulatorne politike NGN-a“, projekt „Pogled u budućnost“, treći kvartal 2012.
- [3] D. Katusic, A. Marcev, R. Vulas i G. Jezic, „Machine-to-Machine: Emerging market and consequences on existing regulatory framework“, *Proceedings of the 12th International Conference on Telecommunications*, Zagreb, Croatia, 2013.
- [4] S-Y. Lien, K-W. Chen i Y. Lin: „Towards Ubiquitous Massive Accesses in 3GPP Machine-to-Machine Communications“, *IEEE Communication Magazine*, vol. 49(4), pp. 66-74, 2011.
- [5] „Machine-to-Machine: Rise of the Machines“, Juniper Networks, 2011.
- [6] 3GPP Technical Specification 22.368, v13.0.0, 3GPP, 2014.
- [7] „Advancing LTE migration heralds massive change in global M2M modules markets“, Machina Research, 2014.
- [8] „Mobile Broadband Connected Future: From Billions of People to Billions of Things“, Yankee Group, 2011.
- [9] Restriction of Hazardous Substances Directive (“Directive 2002/95/EC”), <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:037:0019:0023:en:PDF>, 2003.

- [10] Waste Electrical and Electronic Equipment Directive (“Directive 2002/96/EC”), <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:037:0024:0038:en:PDF>, 2003.
- [11] Radio Equipment and Telecommunications Terminal Equipment and the Mutual Recognition of their Conformity Directive (“Directive 1999/5/EC”), <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1999:091:0010:0010:EN:PDF>, 1999.
- [12] D. Boswarthick, O. Elloumi i O. Hersent: “M2M Communications: A Systems Approach”, Wiley, 2012.
- [13] „M2M/IoT Application Platforms will disrupt traditional M2M platform markets and speed market growth“, Machina Research, 2014.
- [14] Xively, [https://xively.com/whats\\_xively/](https://xively.com/whats_xively/)
- [15] ThingWorx, <http://www.thingworx.com/>
- [16] Bosch, <http://www.bosch-si.com/products/bosch-software-innovations-suite/m2m/device-management.html>
- [17] „Regulation has the potential to disrupt the growth of the Internet of Things – survey“, Machina Research, 2014.
- [18] “EU Directive 2002/58/EC”, Internet: <http://eur-lex.europa.eu/lexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML>, 2002.

## 10. Širokopojasni pristup Internetu u ruralnim područjima

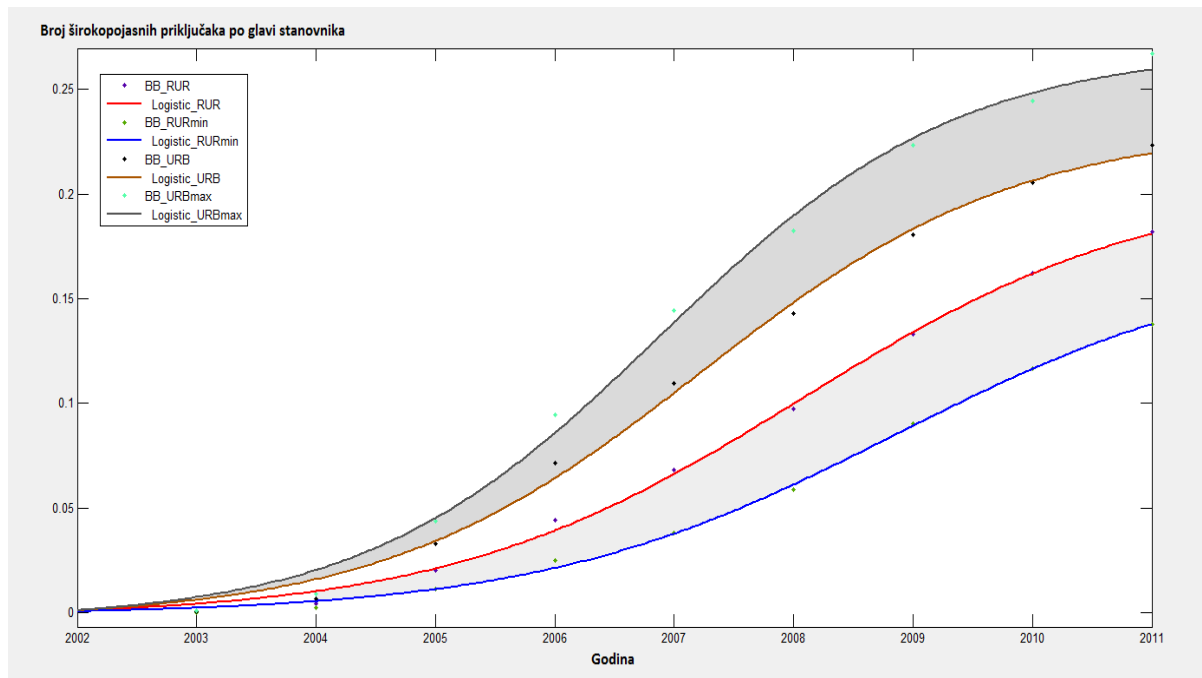
prof.dr.sc. Drago Žagar, dr.sc. Višnja Križanović, dr.sc. Krešimir Grgić, Goran Horvat, mag.ing Sveučilište J.J. Strossmayera u Osijeku, Elektrotehnički fakultet

### 10.1. Analiza digitalnog jaza između ruralnih i urbanih područja

Danas postoje značajne razlike u razinama dostupnosti i stupnju primjene širokopojasnih tehnologija i usluga u ruralnim područjima u odnosu na urbana područja, odnosno prisutan je tzv. digitalni jaz, čiji je intenzitet moguće utvrditi.

Provedena analiza dostupnih podataka o prosječnom broju širokopojasnih priključaka po glavi stanovnika u ruralnim i urbanim područjima u Republici Hrvatskoj ukazala je na postojeće stope usvajanja širokopojasnih usluga u ruralnim i urbanim područjima te je omogućila predviđanje ukupnog broja korisnika u navedenim skupinama područja unutar perioda definiranog Digitalnom Agendom, tj. do 2020. godine.

Na slici 2.1. prikazane su prosječne vrijednosti broja širokopojasnih priključaka po glavi stanovnika u hrvatskim ruralnim ( $BB_{RUR}$ ) i urbanim ( $BB_{URB}$ ) županijama, minimalne vrijednosti u ruralnim županijama ( $BB_{RURmin}$ ), maksimalne vrijednosti u urbanim županijama ( $BB_{URBmax}$ ) te pripadne logističke funkcije (*Logistic*). Prikazane prosječne, maksimalne i minimalne vrijednosti ukazuju na postojanje digitalnog jaza.



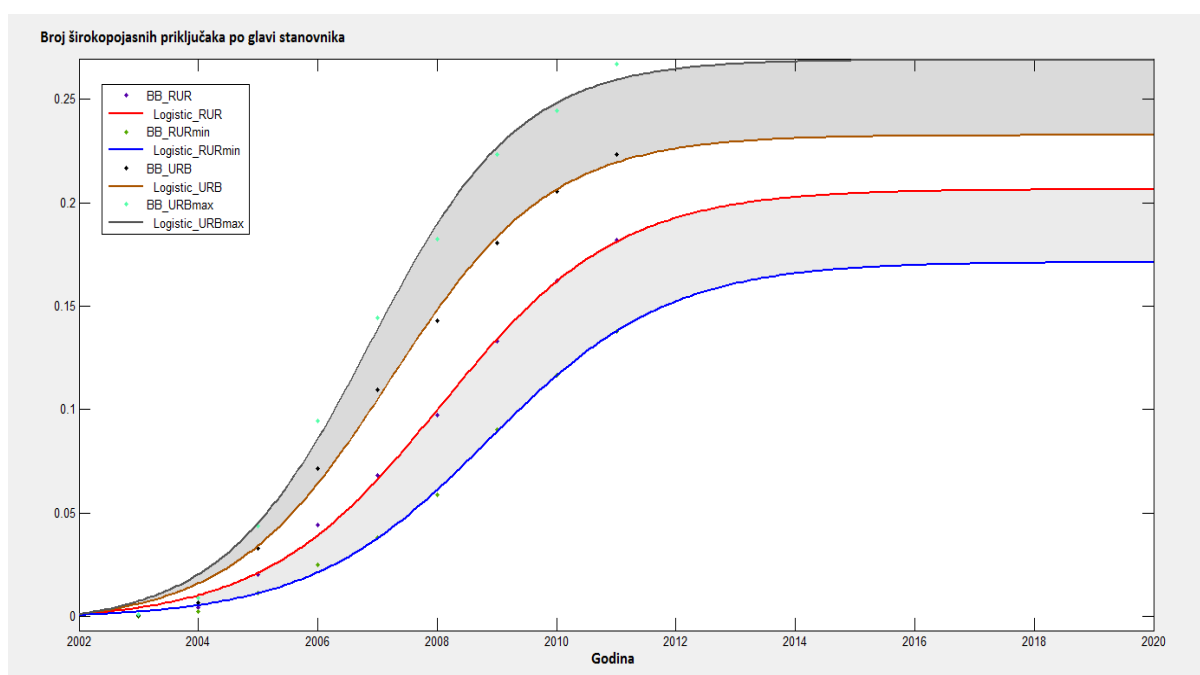
Slika 2.1. Digitalni jaz između ruralnih i urbanih županija

Na temelju podataka o prosječnom broju širokopojasnih priključaka po glavi stanovnika u urbanim županijama, ruralnim županijama te Republici Hrvatskoj procijenjeni su parametri

logističkih funkcija pomoću kojih je opisan broj korisnika širokopojasnog Interneta u ruralnim i urbanim područjima.

Prema dobivenim rezultatima moguće je zaključiti da je parametar koji prikazuje dugoročnu procjenu broja širokopojasnih priključaka veći u urbanim nego u ruralnim županijama. Dugoročno gledano, prosječan broj širokopojasnih priključaka u urbanim županijama teži prema 24%, dok u ruralnim županijama teži prema 21%.

Nadalje, s obzirom na činjenicu da je dobivena vrijednost parametra koji određuje brzinu porasta broja korisnika, veći u urbanim nego u ruralnim županijama, može se zaključiti kako niti u jednom budućem trenutku ruralne županije ne mogu dostići prosjek broja širokopojasnih priključaka po glavi stanovnika istovjetan onom u urbanim županijama u promatranom periodu, kako je prikazano i na slici 2.2.



**Slika 2.2.** Procjena broja širokopojasnih priključaka po glavi stanovnika u ruralnim i urbanim županijama

Dakle, rezultati ukazuju na postojanje digitalnog jaza između ruralnih i urbanih područja, te na činjenicu da, ukoliko se nastave prikazani trendovi porasta broja korisnika širokopojasnog Interneta, jaz između ruralnih i urbanih područja neće biti moguće premostiti. Stoga se nameće zaključak kako je nužno primijeniti odgovarajuće mjere te kreirati modele koji bi trebali potaknuti intenzivniju primjenu širokopojasnih usluga u ruralnim područjima.

## 10.2. Smjernice za smanjenje digitalnog jaza

S obzirom na postojeću situaciju, smanjenju digitalnog jaza moguće je pridonijeti kroz:

- Poticanje daljnjeg **digitalnog opismenjavanja** ruralnog stanovništva;

- Poticanje daljnjeg **usvajanja širokopojasnih pristupnih tehnologija i usluga** kroz razvoj novih aplikacija i usluga prilagođenih zahtjevima i potrebama stanovnika ruralnih područja (takve aplikacije i usluge korisnicima bi trebale omogućiti jednostavniju komunikaciju, pristup važnim elektroničkim informacijskim uslugama, stjecanje novih znanja kroz primjenu on-line edukacijskih sadržaja, rad na daljinu i sl.);
- Poticanje daljnje **implementacije i razvoja širokopojasne pristupne infrastrukture** (stoga je nužno **utvrditi najbitnije čimbenike** koji su u ruralnim područjima povezani s implementacijom širokopojasnog pristupa Internetu, **odabrati najprikladnija širokopojasna pristupna rješenja** za ruralna područja i omogućiti njihovu daljnju implementaciju, kroz čega bi se trebalo ostvariti povećanje ukupnog broja korisnika širokopojasnog pristupa te smanjenje postojećeg digitalnog jaza).

### **10.3. Analiza čimbenika koji utječu na usvajanje širokopojasnih tehnologija i usluga te na uvođenje širokopojasnog pristupa u ruralnim područjima**

Budući da su pri uvođenju širokopojasnog pristupa Internetu troškovi po stanovniku u ruralnim područjima uglavnom veći od troškova po stanovniku u urbanim područjima, ali da je pristup u ruralnim područjima nužan pokretač ekonomskog razvoja područja te da je razvoj ruralnih područja ključan za razvoj ostatka države, osim kriterija koji vrednuju samo isplativost uvođenja širokopojasnog pristupa Internetu, potrebno je voditi računa i o nužnosti uvođenja širokopojasnog pristupa u ruralna područja.

Stoga je potrebno definirati najbitnije kriterije za vrednovanje uvođenja širokopojasnog pristupa Internetu u ruralnim područjima. Takvi kriteriji trebali bi biti zasnovani na provedenim analizama ključnih čimbenika bitnih za uvođenje širokopojasnog pristupa u ruralnim područjima te uključivati interese, kako samih operatora, tako i potencijalnih krajnjih korisnika. Stoga je nužna provedba analize koja ukazuje na čimbenike koji imaju značajan utjecaj na usvajanje i uvođenje širokopojasnog pristupa u ruralnim područjima.

Na dostupnost širokopojasnog pristupa Internetu na određenom području utječe veliki broj različitih čimbenika. Stoga je prilikom razmatranja mogućnosti i opravdanosti uvođenja širokopojasnih pristupnih rješenja u pojedinim područjima potrebno načiniti sustavnu analizu svih čimbenika bitnih za njegovo uvođenje.

Neke do sada provedene studije i analize, navode različite **socio-demografske i tehničke čimbenike** koji utječu na potražnju za širokopojasnim uslugama. Oni uključuju čimbenike poput razine i raspodjele dohotka po glavi stanovnika, dobne strukture stanovništva, razine obrazovanja stanovništva, razine opremljenosti kućanstava informatičkom opremom i razine informatičke pismenosti stanovništva.

Jedan od ključnih **ekonomskih čimbenika** koji utječe na uvođenje širokopojasnog pristupa svakako je i izdatak za nabavu te postavljanje potrebne pristupne mrežne infrastrukture. Dakle, cijena implementacije širokopojasne infrastrukture smatra se ključnim čimbenikom pri



donošenju odluka o uvođenju širokopojasnog pristupa, dok se pri tome, gustoća stanovništva smatra osnovnim čimbenikom koji utječe na cijenu implementacije širokopojasne infrastrukture po korisniku. U slabije naseljenim područjima stanovništvo nije gusto koncentrirano na malim površinama, pa su fiksne pristupne linije koje povezuju lokalne centrale s krajnjim korisnicima u takvim područjima dulje nego u gusto naseljenim područjima. Isto tako, u slabije naseljenim područjima manji broj pretplatnika dijeli trošak implementacije zajedničke opreme. Iz navedenih je razloga cijena izgradnje fiksnih pristupnih širokopojasnih mreža u tim područjima viša u odnosu na gusto naseljena područja. Slično, i troškovi izgradnje mobilnih bežičnih pristupnih širokopojasnih mreža po korisniku su u slabije naseljenim područjima viši, budući da relativno mali broj krajnjih korisnika snosi troškove postavljanja potrebnih pristupnih kapaciteta.

Osim navedenih razloga, i razlike u zemljopisnim značajkama terena, odnosno **geografski čimbenici**, također mogu utjecati na razlike u troškovima implementacije širokopojasnog pristupa te u njegovoj dostupnosti. Tako je, primjerice, zbog nepristupačnijih terena obično skuplje graditi mrežu u planinskim nego u nizinskim područjima.

Nadalje, i **regulatorni čimbenici** utječu na uvođenje širokopojasnog pristupa. Razina konkurencije među operatorima također utječe na cijenu implementacije širokopojasnog pristupa. U pravilu bi povećanje broja operatora koji konkuriraju na istom tržištu trebalo smanjiti cijene uvođenja širokopojasnog pristupa. Međutim, u slabije naseljenim područjima često ne postoji potreba za izgradnjom većeg broja različitih pristupnih mreža. Nadalje, na potražnju za širokopojasnim pristupom Internetu može utjecati i država određenim regulatornim mjerama. Potražnju je moguće potaknuti, dodjeljivanjem poticaja za pretplate na širokopojasni pristup Internetu korisnicima sa nižim primanjima te organiziranjem besplatnih obuka stanovništva u digitalnom opismenjavanju. Nadalje, širokopojasne usluge moguće je popularizirati omogućavanjem jednostavnog pristupa internetskim uslugama i informacijama određenih državnih službi. Država može utjecati na uvođenje širokopojasnog pristupa uključivanjem u izgradnju širokopojasne mreže koja bi ostala u njenom vlasništvu ili pružanjem financijske potpore operatorima za izgradnju širokopojasnih mreža u područjima u kojima ne postoje dostatni poslovni interesi za to. Moguće je i smanjivanje troškova implementacije širokopojasnog pristupa ponudom poreznih olakšica i pojednostavljenjem postupaka za dobivanje prava pristupa postojećoj mrežnoj infrastrukturi. Konačno, moguć je i utjecaj na povećanje konkurentnosti među operatorima kroz smanjivanje regulatornih prepreka za ulazak novih operatora na tržište ili kroz postavljanje zahtijeva za dijeljenjem infrastrukture pred one operatore koji imaju monopol na tržištu. Povećanje broja širokopojasnih priključaka u ruralnim područjima moguće je poticati kroz definiranje optimiziranih poslovnih modela koji će stimulirati uvođenje cjenovno prihvatljivih širokopojasnih rješenja na regionalnim i lokalnim razinama.

Osim navedenih socio-demografskih, geo-ekonomskih i regulatornih čimbenika, na uvođenje širokopojasnog pristupa Internetu utječu i **drugi čimbenici**, npr. razina razvijenosti već postojeće telekomunikacijske infrastrukture, način na koji su na određenom području raspoređene platforme za žični i bežični širokopojasni pristup te raznolikost postojeće ponude usluga mobilnog i fiksnog širokopojasnog pristupa i interes korisnika za navedene usluge i dr.

#### **10.4. Prijedlog i izrada tehno-ekonomskog modela koji se zasniva na rezultatima provedenih analiza**

Tehno-ekonomski modeli primjenjuju se pri vrednovanju implementacije pojedinih širokopojasnih pristupnih rješenja, pri izboru optimalnih pristupnih rješenja te pri izboru najpogodnijeg trenutka za investiranje.

Kada se pri izboru tehnologija promatraju manja ruralna područja, scenariji koji obuhvaćaju različite tipove ruralnih naselja – osamljena gospodarstva, disperzna sela te prigradska naselja, rezultati brojnih provedenih analiza navode na zaključke definirane u nastavku.

- **U osamljenim gospodarstvima** analiza kapitalnih izdataka, godišnjih troškova i trenutne vrijednosti u određenom periodu, pokazuje da su među najisplativijim tehnološkim rješenjima WiMAX i PLC. WiMAX predstavlja pristupno rješenje koje je, zbog veće širine frekvencijskog pojasa i niže cijene, konkurentnije od satelitskog pristupa. Premda se 3G/4G mobilni radijski pristup čini skupim, njegova se cijena smanjuje ukoliko je postavljen dio potrebne pristupne infrastrukture. Izgradnja nove fizičke infrastrukture potrebna za HFC i FTTU tehnologije je skupo rješenje. Budući da je nadogradnja HFC-a, zbog nepostojanja ranije izgrađene infrastrukture kableske televizije, nemoguća, ova je tehnologija isključena pri analizi osamljenih gospodarstava.
- **U disperznim selima** analiza pokazuje da su među najisplativijim rješenjima WiMAX, ADSL i PLC tehnologije. Naravno, uvođenje HFC-a uz nadogradnju kableske infrastrukture je, na ograničenom broju područja u kojima ona od ranije postoji, isplativije rješenje nego uvođenje HFC-a uz postavljanje nove infrastrukture. Međutim, HFC je svakako skupo rješenje. Izgradnja nove fizičke infrastrukture potrebne za FTTU tehnologiju ima najvišu cijenu.
- **U malim gradićima – prigradskim naseljima** među najisplativijim rješenjima nalazi se ADSL tehnologija. Najskuplje rješenje je uvijek postavljanje nove infrastrukture. Zato se nadogradnji HFC-a u ograničenom području u kojem od ranije postoji kableska infrastruktura, daje prednost.

Dakle, kao zaključak moguće je izdvojiti da su u svim promatranim tipovima ruralnih naselja među najisplativijim pristupnim rješenjima ADSL, WiMAX i PLC te 3G/4G.

Iako je PLC tehnologija između navedenih fiksnih rješenja najisplativije rješenje, s obzirom na činjenicu da pristup Internetu preko elektroenergetske mreže još uvijek nije dostupan u mnogim europskim državama, pa tako ni u Republici Hrvatskoj, PLC nije uključen u naknadno provedene analize. Dakle, od prikazanih rješenja **za promatrana ruralna područja među najprikladnijim su rješenjima ADSL, WiMAX i 3G/4G tehnologije koje redom predstavljaju fiksna žična, fiksna bežična i mobilna bežična pristupna rješenja.**

### 10.5. Izbor optimalnih širokopojasnih pristupnih rješenja za odabrane ruralne scenarije

Usporedba između skupine žičnih i bežičnih pristupnih tehnologija načinjena je s obzirom na:

- maksimalnu raspoloživu širinu frekvencijskih pojaseva po korisniku unutar skupine,
- maksimalni ostvarivi domet tehnologija unutar razmatrane skupine te
- način implementacije pristupne mrežne infrastrukture.

S obzirom na **maksimalne ostvarive širine frekvencijskih pojaseva** po korisniku, žične su tehnologije u prednosti nad bežičnim rješenjima budući da ostvarive širine frekvencijskih pojaseva bežičnih tehnologija ovise o brojnim čimbenicima, poput udaljenosti od pristupnih točaka te o interferenciji.

Pri usporedbi dometa između navedenih skupina tehnologija bitno je naznačiti da je **maksimalni ostvarivi domet** pojedinih bežičnih rješenja veći u odnosu na maksimalni domet koji je moguće ostvariti žičnim pristupnim rješenjima.

Nadalje, s obzirom na **složenost implementacije mrežne infrastrukture** i na činjenicu da je za žična rješenja nužna izgradnja ili nadogradnja žične pristupne infrastrukture, implementacija bežičnih rješenja je jednostavnija.

Nadalje, rezultati provedenih tehno-ekonomskih analiza uvođenja fiksnih žičnih (ADSL), fiksnih bežičnih (WiMAX) te mobilnih bežičnih (UMTS) širokopojasnih pristupnih rješenja nameću sljedeće zaključke:

- usporedba isplativosti različitih **fiksnih pristupnih tehnologija** ukazala je na činjenicu da u cilju povećanja isplativosti fiksnog pristupa treba iskoristiti svu dostupnu mrežnu infrastrukturu
- usporedba isplativosti **mobilnih i fiksnih pristupnih tehnologija** ukazala je na činjenicu da u odnosu na fiksna pristupna rješenja (ADSL i WiMAX) mobilna rješenja (WiMAX i LTE) općenito imaju duži period povrata inicijalnih ulaganja
- usporedba isplativosti **žičnih i bežičnih pristupnih tehnologija** ukazala je na činjenicu da su u slučajevima kada je moguća nadogradnja postojeće žične infrastrukture, nadograđena žična rješenja (ADSL) općenito isplativija u odnosu na nova bežična pristupna rješenja (WiMAX)
- međutim, nove **mobilne mreže** (mobilni WiMAX) **predstavljaju ekonomski prihvatljivo rješenje kada nije dostupna fiksna infrastruktura koju je moguće nadograditi** (fiksni WiMAX).

## 10.6. Postupci pri tehno-ekonomskom modeliranju

Pri analiziranju tehno-ekonomskih aspekata uvođenja širokopojasnog pristupa Internetu i internetskih usluga u ruralna područja potrebno je razmotriti postojeću problematiku. U razmatrane aspekte ubrajaju se različiti tržišni, tehnički i ekonomski aspekti. Pojedini postupci primijenjeni za rješavanje navedene problematike objašnjeni su kroz primjer tehno-ekonomske analize uvođenja bežičnog širokopojasnog pristupa Internetu (fiksno i mobilno) u ruralna područja.

### A) Tržišni aspekti:

#### *Definiranje industrijskih arhitektura:*

S obzirom na veliki broj različitih sudionika na telekomunikacijskim tržištima, prije provedbe samih analiza potrebno je definirati ciljne skupine za koje se utvrđuje opravdanost uvođenja širokopojasnog pristupa Internetu. Budući da bez potrebne pristupne infrastrukture ne postoji mogućnost primjene širokopojasnih usluga, opravdanost uvođenja širokopojasnog pristupa Internetu potrebno je analizirati prvenstveno s gledišta mrežnih operatora. Takve je analize potrebno provoditi s ciljem procjenjivanja ekonomske isplativosti implementacije razmatranih tehničkih rješenja, odnosno širokopojasnih pristupnih mreža. Provedba tehno-ekonomskih analiza uvođenja širokopojasnog pristupa Internetu za mrežne operatore u odabranim ruralnim područjima treba uključivati veći broj različitih pristupnih tehnologija. Analiza različitih tehnologija omogućuje bolji uvid u dostupna rješenja te olakšava izbor najprikladnijih rješenja u pojedinim tipovima ruralnih područja, kako je u nastavku prikazano za fiksna i mobilna bežična pristupna rješenja.

#### *Definiranje scenarija:*

Prije provedbe tehno-ekonomskih analiza potrebno je odabrati prikladne scenarije u kojima je potrebno provesti analize budući da izbor najprikladnijih širokopojasnih pristupnih rješenja uvelike ovisi o odabranom scenariju. Nakon izbora scenarija potrebno je prikupiti i analizirati podatke o razmatranom području (npr. geografske i demografske podatke). Primjer definiranja scenarija opisan je u tablici 2.1.

**Tablica 2.1.** Definiranje promatranog područja i izbor scenarija

Promatrano područje	Površina [ $km^2$ ]		Demografski podaci
	Ukupno područje	Ciljno područje	Ukupan broj kućanstava
<b>Odabrani ruralni scenarij</b>	40	32	1.903

#### *Modeliranje tržišta:*

Pri modeliranju tržišta potrebno je predvidjeti dinamiku usvajanja tehnologija i usluga u promatranom scenariju. Pri tome je potrebno u obzir uzeti i podatke o udjelu postojećih operatora na tržištu koji nude istovrsne usluge. Uz pretpostavku o podjeli tržišta između više

operatora, u odabranom scenariju prikazanom u tablici 2.1., definirano ciljno područje pokrivenosti uslugom manje je u odnosu na ukupno područje.

Nadalje, s obzirom na udio operatora na tržištu, pri procjeni ciljnog broja kućanstava koja trebaju biti pokrivena uslugom određen je njihov udio u ukupnom broju kućanstava, kako je prikazano u tablici 2.2. Za procjenu broja kućanstava u godinama unutar definiranog perioda promatranja potrebno je primijeniti neki od modela koji predviđaju usvajanje novih usluga (npr. logistički model - primijenjen pri određivanju podataka prikazanih u tablici). Pri tome je pri predviđanju moguće koristiti dostupne povijesne podatke o brzini usvajanja istovrsnih ili sličnih usluga.

**Tablica 2.2.** Definiranje razmatranog tržišnog segmenta

Ciljani tržišni segment i zahtjevi za kapacitetom u odabranom scenariju											
Period promatranja (godine)		G1	G2	G3	G4	G5	G6	G7	G8	G9	G10
Ukupni ciljni broj kućanstava		27	42	67	90	123	155	180	199	211	217
Ukupni zahtjevi za kapacitetom	Dolazni smjer [Mbit/s]	0,58	0,90	1,43	1,92	2,62	3,31	3,84	4,25	4,50	4,63
	Odlazni smjer [Mbit/s]	0,29	0,45	0,71	0,96	1,31	1,65	1,92	2,12	2,25	2,31

## B) Tehnički aspekti:

### *Planiranje pristupnih mreža:*

Ovisno o vrstama analiziranih tehnologija za širokopojasni pristup, pri provedbi tehničkog dijela tehno-ekonomskih analiza potrebno je posebno razmotriti problem izbora prikladnih modela za planiranje pristupnih mreža. Ovisno o tome radi li se o žičnom ili bežičnom pristupu te o razmatranoj vrsti tehnologija (fiksne/mobilne), metode modeliranja pristupnih mreža potrebno je prilagoditi i samom scenariju, odnosno tipu ruralnog područja. Pri planiranju pristupnih mreža posebnu je pažnju potrebno posvetiti određivanju količine potrebnih mrežnih komponenata kako bi bili zadovoljeni ukupni zahtjevi za kapacitetom.

Tako je načinjeno i u primjeru iz tablice 2.3. u kojem je određen potreban broj WiMAX baznih stanica za različite podscenarije označene oznakama SA, SB, SC i SF (ovisno o dostupnim širinama frekvencijskih kanala, tehnikama kodiranja i načinu prijenosa podataka) unutar scenarija definiranog u tablici 2.1.

Pri tome je ukupne zahtjeve za kapacitetom potrebno je proračunati na temelju podataka o prosječnim zahtjevima za kapacitetom po korisniku te o ukupnom broju korisnika (kućanstava) u pojedinom vremenskom razdoblju, kako je prikazano u tablici 2.3.

Tablica 2.3. Planiranje pristupne mreže

Broj potrebnih baznih stanica za implementiranje odabrane WiMAX pristupne mreže u definiranom scenariju												
Mobilni WiMAX										Fiksni WiMAX		
Širina frekvencijskog kanala, multipleksiranje:	Višestruki prijenos:	Broj antena (odašiljanje /prijem):	Tehnike kodiranja:	Ozn. scenarija:	Frekv. pojas:	Ozn. scenarija:	Frekv. pojas:	Ozn. scenarija:	Frekv. pojas:	Širina frekvencijskog kanala, multipleksiranje:	Ozn. scenarija:	Frekv. pojas:
					2.3 GHz		2.5 GHz		3.5 GHz			
5 MHz, TDD	-	1 x 1	-	SA-01	3	SB-01	3	SC-01	3	3.5 MHz, TDD or FDD	SF-01	7
	MIMO	1 x 2	-	SA-02	2	SB-02	2	SC-02	3		SF-02	5
			Matrix A (STC)	SA-03	2	SB-03	2	SC-03	3		SF-03	5
		2 x 2	-	SA-04	3	SB-04	3	SC-04	3		SF-04	7
			Matrix A (STC)	SA-05	2	SB-05	2	SC-05	2		SF-05	4
	10 MHz, TDD	-	1 x 1	-	SA-06	4	SB-06	4	SC-06		5	7 MHz, TDD or FDD
MIMO		1 x 2	-	SA-07	3	SB-07	3	SC-07	3	SF-07	7	
			Matrix A (STC)	SA-08	3	SB-08	3	SC-08	3	SF-08	7	
		2 x 2	-	SA-09	4	SB-09	4	SC-09	5	SF-09	9	
			Matrix A (STC)	SA-10	2	SB-10	2	SC-10	3	SF-10	5	

*Planiranje nadogradnje postojeće mrežne infrastrukture:*

Kroz tehnički dio tehno-ekonomskih analiza potrebno je definirati modele i provesti planiranje pristupnih mreža za različite tehnologije. Budući da je prilikom razmatranja različitih pristupnih rješenja potrebno razmotriti i činjenicu da ne zahtijevaju sva rješenja pri implementaciji jednake postupke, pristupna rješenja je nužno razlikovati prema potrebnim ulaganjima u pristupnu infrastrukturu, ovisno o tome postoji li mogućnost za nadogradnju postojeće infrastrukture ili je potrebna u potpunosti nova infrastruktura. Uvijek kada je moguće, potrebno je nadograditi postojeći dio pristupne infrastrukture budući da su tada potrebna manja ulaganja.

### **C) Ekonomski aspekti:**

#### *Definiranje troškova:*

Pri provedbi ekonomskog dijela tehno-ekonomskih analiza, u svrhu procjene izdataka pri uvođenju širokopojasnog pristupa, potrebno je definirati razlike između izdataka ovisno o njihovom opsegu te vremenu u kojem nastaju. Izdatke je potrebno podijeliti na jednokratne i godišnje te kapitalne i operativne.

#### *Određivanje cijene mrežne opreme:*

Pri provedbi tehno-ekonomskih analiza često se javlja problem određivanja cijene mrežne opreme koja se koristi u analizama budući da podaci mogu biti preuzeti iz različitih izvora. Stoga je potrebno na temelju svih prikupljenih dostupnih podataka odrediti prosječne iznose cijena opreme i njih uključiti u izračune, a nakon toga u analizu uključiti i raspon mogućih vrijednosti cijena uz primjenu neke od raspodjela vjerojatnosti.

#### *Definiranje perioda ulaganja:*

Prije provedbe ekonomskog dijela tehno-ekonomskih analiza nužno je definirati i odgovarajuće vremenske periode unutar kojih se vrše kapitalna ulaganja budući da je ulaganja u mrežnu infrastrukturu moguće vršiti jednokratno ili unutar dužeg vremenskog perioda, što utječe na konačne periode isplativosti projekata. Ukoliko se pristupne mreže grade korak po korak moguće je ograničiti rizike i povećati operativnu fleksibilnost projekta jer je na temelju naknadnog odgovora dobivenog s tržišta moguće odlučiti hoće li i u kojem roku mreža biti nadograđena.

#### *Prikazivanje rezultata:*

Pri ocjenjivanju ekonomske isplativosti ulaganja u širokopojasnu infrastrukturu, rezultate je moguće prezentirati na različite načine. Navedeni problem potrebno je riješiti izborom najprikladnijih načina za prezentiranje rezultata. Najčešće su to mjere isplativosti koje obuhvaćaju period povrata ulaganja, neto sadašnje vrijednosti ulaganja i unutarnje stope povrata ulaganja.

#### *Analiziranje osjetljivosti:*

Kako bi problem nesigurnosti procjena dobivenih rezultata analiza bio što manji, potrebno je provesti analize osjetljivosti. One mogu uključivati pretpostavke o različitim pokrivenostima područja uslugom, zahtijevanim kapacitetima i primijenjenim diskontnim stopama u razmatranim scenarijima i sl.

**Tablica 2.4.** Procjena isplativosti različitih pristupnih rješenja

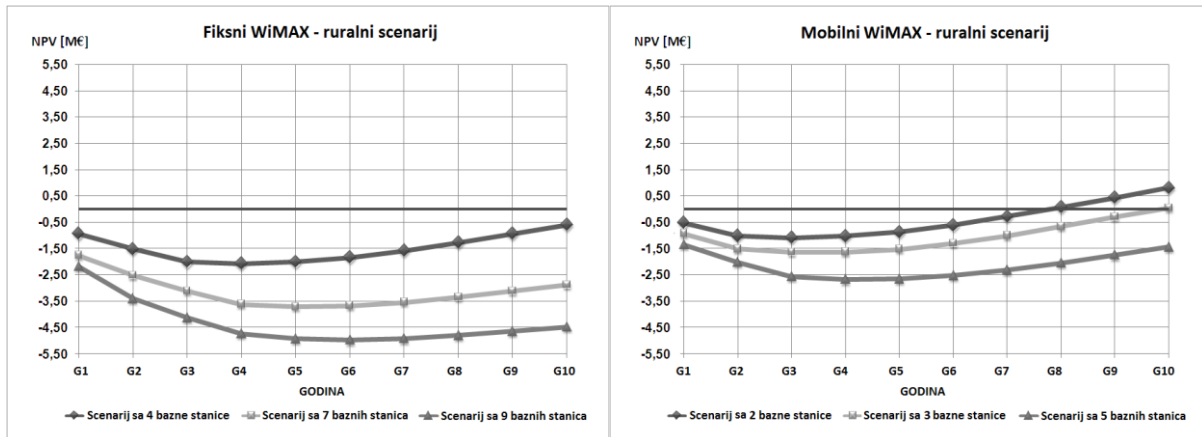
Neto sadašnje vrijednosti [€]												
u scenariju u kojem se razmatra uvođenje mobilne WiMAX pristupne infrastrukture												
Usporedba:	Oznaka scenarija:	Broj baznih stanica:	G1	G2	G3	G4	G5	G6	G7	G8	G9	G10
Širina frekventijskog kanala	SC-05	2	-52,333	-102,025	-108,962	-103,331	-87,655	-61,744	-28,285	6,653	43,435	80,106
	SC-10	3	-93,720	-152,087	-164,330	-163,658	-152,616	-131,036	-101,444	-66,907	-30,059	3,892
Tehnike kodiranja	SC-09	5	-135,108	-202,149	-255,847	-267,710	-265,937	-253,020	-231,524	-204,552	-174,776	-144,414
	SC-10	3	-93,720	-152,087	-164,330	-163,658	-152,616	-131,036	-101,444	-66,907	-30,059	3,892
Način prijenosa	SC-06	5	-135,108	-202,149	-255,847	-267,710	-265,937	-253,020	-231,524	-204,552	-174,776	-144,414
	SC-07	3	-93,720	-152,087	-164,330	-163,658	-152,616	-131,036	-101,444	-66,907	-30,059	3,892
Neto sadašnje vrijednosti [€]												
u scenariju u kojem se razmatra uvođenje fiksne WiMAX pristupne infrastrukture												
Usporedba:	Oznaka scenarija:	Broj baznih stanica:	G1	G2	G3	G4	G5	G6	G7	G8	G9	G10
Širina frekventijskog kanala	SF-05	4	-93,720	-152,087	-200,479	-207,384	-200,977	-183,728	-158,184	-127,429	-94,117	-60,451
	SF-10	5	-135,108	-202,149	-255,847	-267,710	-265,937	-253,020	-231,524	-204,552	-174,776	-144,414
Tehnike kodiranja	SF-09	9	-217,882	-340,952	-413,369	-473,893	-493,104	-497,511	-492,207	-480,368	-464,733	-447,588
	SF-10	5	-135,108	-202,149	-255,847	-267,710	-265,937	-253,020	-231,524	-204,552	-174,776	-144,414
Način prijenosa	SF-06	9	-217,882	-340,952	-413,369	-473,893	-493,104	-497,511	-492,207	-480,368	-464,733	-447,588
	SF-07	7	-176,495	-252,211	-311,214	-361,821	-371,764	-367,508	-354,108	-334,703	-311,997	-288,244

*Analiziranje rizika:*

Nakon utvrđivanja ključnih čimbenika koji određuju isplativost ulaganja u širokopoljasnu infrastrukturu, u cilju smanjivanja rizika nesigurnosti procjene isplativosti u pojedinim scenarijima, potrebno je provesti analize rizika za ključne parametre, tj. za one parametre koji najviše utječu na konačnu cijenu širokopoljasnih rješenja.

Tako je načinjeno i u primjeru u tablici 2.4., gdje su prikazani različiti iznosi neto sadašnjih vrijednosti, ovisni o količini mrežne opreme koju uvjetuju razlike u dostupnim širinama frekventijskih kanala, primijenjenim tehnikama kodiranja i načinima prijenosa podataka u mobilnoj te u fiksnoj WiMAX mreži.





**Slika 2.3.** Usporedba isplativosti fiksnih i mobilnih bežičnih pristupnih rješenja

## 10.7. Zaključna razmatranja

Na posljetku, moguće je istaknuti sljedeće:

- U ruralnim područjima u kojima nije dostupna žična pristupna infrastruktura, bežična pristupna rješenja predstavljaju alternativni način pristupa Internetu.
- U usporedbi sa žičnim rješenjima, bežična pristupna rješenja imaju brojne prednosti, prije svega, mobilnost, kompatibilnost te mogućnost osiguravanja odgovarajućih razina kvalitete usluga pri naglom porastu zahtjeva za širokopojsnim uslugama.
- Stoga je provedena analiza i usporedba implementacije različitih bežičnih pristupnih rješenja.
- Kako bi se omogućile sve prednosti bežičnog širokopojsnog pristupa, za bežične internetske usluge nužno je osigurati dostatnu količinu spektra. Stoga je dodjela spektra za širokopojsne usluge vrlo bitan korak u procesu implementacije bežičnog pristupa Internetu. Dostupnost i način dodjele spektra ključan je element pri implementaciji bežičnih rješenja te će uvjetovati njihov budući razvoj.
- Mobilne bežične širokopojsne tehnologije predstavljaju ekonomično pristupno rješenje za rijetko naseljena ruralna područja te za područja u kojima ne postoji dostupna žična pristupna rješenja.
- U cilju optimizacije pristupnih rješenja za ruralna područja, provedena je analiza i usporedba fiksnih i mobilnih bežičnih rješenja na primjeru WiMAX tehnologije.
- Pri provedbi analize osjetljivosti razmotrene su razlike u dostupnim širinama frekvencijskih kanala (5 MHz i 10 MHz za mobilni WiMAX, te 3.5 i 7 MHz za fiksni WiMAX) na različitim dostupnim frekvencijskim pojasima (2.3 GHz pojas, 2.5 GHz pojas te pojas dostupan u Republici Hrvatskoj - 3.5 GHz), primijenjenim tehnikama kodiranja (engl. *Space Time Coding*, STC) i načinima prijenosa podataka u pristupnoj

WiMAX mreži (po jedna ili više antena na predajnoj i prijemnoj strani) na isplativost pristupnih rješenja.

- Dobiveni rezultati ukazuju na činjenicu da su najprikladniji scenariji za povećanje isplativosti pristupnih rješenja u ruralnim područjima scenariji u kojima se koriste manje širine frekvencijskih kanala (tj. 5 MHz kanal za mobilni WiMAX te 3.5 MHz za fiksni WiMAX). Nadalje, rezultati ukazuju i na činjenicu da je preporučljiva primjena tehnika kodiranja koje povećavaju dometa bežičnog signala.
- U usporedbi s fiksnim scenarijima (SF), mobilni WiMAX scenariji (SC) zahtijevaju pri radu manji broj baznih stanica u istom frekvencijskom pojasu.
- Smanjenje broja baznih stanica smanjuje ukupne troškove nužne za implementaciju WiMAX pristupnih rješenja, neovisno o većem potrebnom broju antena na predajnoj i prijemnoj strani.
- Dakle, nove mobilne mreže (mobilni WiMAX) predstavljaju ekonomski prihvatljivo rješenje kada nije dostupna fiksna infrastruktura koju je moguće nadograditi (fiksni WiMAX), kako je prikazano usporedbom dobivenih rezultata prikazanih na slici 2.3.

## **11. Usluge za osobe sa složenim komunikacijskim potrebama - pristupačnost ICT usluga i osobe starije dobi**

izv.prof.dr.sc. Željka Car  
Sveučilište u Zagrebu, Fakultet elektrotehnike i računarstva

### **11.1. Uvod**

Stupanj socijalne uključenosti osoba sa složenim komunikacijskim potrebama moguće je povećati razvojem ICT usluga koje će im omogućiti efikasniju komunikaciju, dostup informacijama i pružiti podršku pri edukaciji [1]. Pristup informacijskim i komunikacijskim tehnologijama je po Konvenciji Ujedinjenih naroda o pravima ljudi s invaliditetom<sup>35</sup> priznat kao osnovno ljudsko pravo.

Pojam e-Pristupačnost (engl. *e-Accessibility*) označava nastojanje da ICT usluge budu dostupne i prihvatljive za korištenje osobama s invaliditetom kao i osobama starije životne dobi koje imaju smanjene komunikacijske mogućnosti, bez potrebe za dodatnim alatima, tehnologijama ili uređajima. Kako bi ICT proizvodima i uslugama mogli pristupati i koristiti ih ravnopravno svi korisnici bez obzira na invaliditet ili dob, potrebno je pri osmišljavanju funkcionalnosti, a pogotovo pri dizajniranju korisničkih sučelja voditi računa o mogućnostima i specifičnim potrebama korisnika poput oštećenja vida, sluha, govora, motoričke poremećaje, intelektualne teškoće i neurološke poremećaje. ICT rješenja koja imaju pristupačni dizajn također imaju i dodanu vrijednost s obzirom na općenito poboljšanu uporabljivost te jer olakšavaju korištenje usluga i korisnicima bez poteškoća.

Tehnologije današnjice, pogotovo nove generacija pokretnih uređaja, omogućavaju lako ostvarivanje interakcije korisnika i usluge korištenjem zaslona na dodir te ostalih standardnih ulaznih jedinica (miš, tipkovnica, upravljačka palica itd.). Prednost interakcije putem zaslona na dodir jest intuitivnost i jednostavnost koju takav način interakcije pruža što je korisniku mnogo jednostavnije i prihvatljivije. Mogućnosti koje pruža zaslon na dodir najviše dolaze do izražaja kod malih pokretnih uređaja gdje je ulazna jedinica integrirana u sam uređaj. Sve više se povećava broj korisnika koji sjedištima weba pristupaju putem malih pokretnih uređaja, što postavlja dodatni zahtjev na izvedbu jedinstvenog izgleda i funkcionalnosti korisničkih sučelja.

### **11.2. Složene komunikacijske potrebe i osobe starije dobi**

Osobe sa složenim komunikacijskim potrebama nisu u mogućnosti privremeno ili trajno komunicirati putem govora i/ili imaju teškoće u proizvodnji i/ili razumijevanju oralnog i/ili pisanog jezika.

---

<sup>35</sup> Convention on the Rights of Persons with Disabilities, UN Enable

Starenje stanovništva u svijetu je u porastu i nastavit će se idućih desetljeća: prema procjenama UN-a<sup>36</sup> do 2025. godine bit će oko 1,2 milijarde osoba starijih od 60 i više godina, a do 2050 oko 2 milijarde. Stoga sve veći broj starijih putem usluga weba poboljšava svoje samostalno sudjelovanje u društvu, pri čemu se smatra da su starije osobe najbrže rastući segment korisnika Interneta [2]. Također, starije stanovništvo predstavlja značajan tržišni segment za ICT industriju. Istraživanja načina korištenja računala u starijoj populaciji, mogućnosti prilagodbe postojećih ICT usluga te implementacija novih kako bi se iskoristile mogućnosti suvremenih tehnologija za poboljšanje kvalitete života starijih osoba u zadnje je vrijeme prisutno u različitim područjima poput interakcije čovjeka i računala (engl. *Human Computer Interaction*, HCI), gerontologija, zdravstvo, psihologija i poslovni sektor [3].

U vezi s normalnim procesom starenja su brojne tjelesne, psihofizičke, biološke i socijalne promjene, koje bitno određuju funkcionalne sposobnosti i komunikacijske osobitosti starijih osoba. Te se promjene ne mogu smatrati bolestima pa je stereotip o starijima kao bolesnima i nemoćnim osobama netočan. Također, kako pojedinac stari i/ili mu se pojavljuju određene fizičke/kognitivne poteškoće, društveni izazovi postaju sve vidljiviji. Smanjuje se pokretnost i pristup informacijama. Ekonomski budžet uglavnom je manji. Povećava se osamljenost i depresija te osjećaj isključenosti. U slučaju kada osobe starije dobi iskuse poteškoće koje im otežavaju komuniciranje i samostalno sudjelovanje u društvu, smatraju se osobama sa složenim komunikacijskim potrebama.

Postoje različite definicije tko su osobe starije dobi, pri čemu donja dobna granica varira od 50 do 65 godina. Većina zapadnih zemalja, uključujući SAD, smatra donjom granicom godinu umirovljenja, odnosno 65 godina [4].

Unatoč kronološkoj definiciji starosti, postoji velika raznolikost u sposobnostima/potrebama starijih osoba, koja proizlazi iz razvojnih i funkcijskih ograničenja pridruženih starenju, kao i različiti stav prema starenju. Ovi faktori, kao i sklonost/iskustvo u korištenju ICT rješenja utječu na primjenu i prilagodbu tehnologije, pogotovo ICT rješenja i usluga Weba starijim osobama.

Najčešće poteškoće koje imaju osobe starije dobi jesu:

- Poteškoće vida – smanjena je kontrastna osjetljivost, percepcija boja i otežana fokusiranost na predmete u blizini što otežava čitanje web stranica.
- Motoričke poteškoće – smanjena spretnost i fina motorička kontrola pokreta i tremor što otežava korištenje miša.
- Oštećenje sluha – smanjena osjetljivosti na visoke tonove, poteškoće u razlikovanju osnovne slušne poruke od pozadine te s razumijevanjem brzoga govora.

Kognitivne poteškoće – uključuju smanjeno kratkotrajno pamćenje, poteškoće u koncentraciji i laku smetenost što otežava navigaciju i interakciju s ICT uslugama.

---

<sup>36</sup> Enhancing the voice of older persons, <http://www.un.org/en/development/desa/news/social/older-persons.html>

### 11.3. Osobe starije dobi i korištenje ICT usluga

Korištenje tehnologije u korist i od strane osoba starije dobi predmet je istraživanja dugi niz godina. Pojam *gerotehnologija* označava akademska i profesionalna interdisciplinarna istraživanja koji kombiniraju gerontologiju i tehnologiju s ciljem kreiranja optimalnog životnog okruženja osobama starije dobi s ciljem smanjenja smrtnosti i povećanja vitalnosti te uključuje zdravlje, stanovanje, mobilnost, komunikacije, slobodno vrijeme i rad starijih osoba. Međunarodno društvo za gerotehnologiju osnovano je 1997. godine u Münchenu u svrhu uspostave suradnje i razmjene istraživača, razvijatelja i starijih osoba, kako bi zajedno dizajnirali i implementirali tehnološka rješenja koja će ostvarivati postavljene ciljeve gerotehnologije [5].

Postoji veliki potencijal u primjeni novih ICT tehnologija koje osobama s invaliditetom i starijim osobama omogućuju komunikaciju, pristup informacijama i povećavaju kvalitetu života. Tako na primjer, usluge weba omogućuju [12]:

- održavanje komunikacije s obitelji i rodbinom te proširenje društvene mreže (e-mail komunikacija je često polazna točka za one koji su novi korisnici Interneta)
- pristup komercijalnim uslugama online, uključujući istraživanje proizvoda, kupovinu i bankarstvo, kojima bi stariji mogli teže pristupiti uživo zbog problema pokretljivosti
- pristup informacijama izvršne vlasti i građansko sudjelovanje u raznim procesima odlučivanja
- pristup vijestima, informacijama o sportu, putovanjima, zdravlju i ostalim aktualnim temama
- pronalazak posla i pristup web aplikacijama koje se odnose na zaposlenje tijekom njihovog kasnijeg radnog života (dob umirovljenja se podiže)
- pristup prilikama za vježbanje i učenje – profesionalno ili u slobodno vrijeme i kao hobiji
- nastavak života u svojim domovima, osiguravajući im što dulju neovisnost o drugima.

ICT rješenja imaju posebno značajnu ulogu, jer imaju potencijal povećati osobama starije dobi, osobama s invaliditetom te nemoćnim osobama nezavisnost, mobilnost i sudjelovanje u različitim aspektima svakodnevnog života (slobodno vrijeme, posao, dom, zdravlje, itd.). Postoji sve veći interes za korištenje ICT-a u svrhu poboljšanja kvalitete života starijih osoba i izgradnju pametnih gradova.

Neurodegenerativne bolesti su uglavnom neizlječiva stanja snažno povezana sa starijom dobi. Procjenjuje se da je u Europi postoji između 6,3 i 7,3 milijuna ljudi koji pate od Alzheimerove bolesti i srodnih poremećaja [5] koje spadaju u najčešće neurodegenerativne bolesti. Kako europska populacija ima sve više i više starijih, očekuje se povećanje ovog trenda.

Ozbiljne igre (engl. *Serious games*) predstavljaju nove i potencijalno učinkovite alate u treningu mozga starijih odraslih osoba s blagim kognitivnim oštećenjima (engl. *Mild Cognitive Impairments*, MCI), stanja koje karakterizira blagi kognitivni deficit uz nepostojanje funkcijskog poremećaja. Preliminarni podaci iz literature pokazuju da interaktivno učenje uz pomoć računala, treninzi memorije i uključenost osoba starije dobi u računalne aktivnosti smanjuju šanse za blaga kognitivna oštećenja te u nekim slučajevima smanjuju propadanje kognitivnih sposobnosti pacijenata s Alzheimerovom bolesti i demencijom. [5]

Iako je integracija ICT rješenja u gotovo sve aspekte svakodnevnog života izuzetno korisna, često je na žalost vrlo frustrirajuća i zbunjujuća za osobe s invaliditetom/složenim komunikacijskim poteškoćama i osobe starije dobi. Razlog tome je ponekad narav samog tehnološkog rješenja i korisničko neiskustvo u primjeni tehnologije, ali je najčešće razlog neprilagođeni dizajn korisničkih sučelja i zanemarivanje specifičnih potreba ovih skupina korisnika tijekom razvoja ICT usluga.

Barijere koje osjećaju osobe starije dobi može se ilustrirati primjerom nove generacije pametnih telefona s ekranima na dodir čija korisnička sučelja sadrže jednu ili svega nekoliko sklopovskih tipki. Najčešće početno korisničko sučelje (početni ekran) tih telefona nalikuje početnom ekranu računala, dok je sučelje koje starijim osobama najčešće treba za uspostavu poziva (dial-up sučelje) sadržano unutar nekog izbornika ili sakriveno, što im otežava korištenje i snalaženje. Nadalje, operacijski sustavi, web sjedišta i stranice, web usluge i aplikacije za pokretne uređaje često sadrže izbornike i koriste navigaciju s mnogo ikona.

Također se pojavljuju problemi interakcije s računalnim komponentama. Miševi i tipkovnice se smanjuju, na zaslonima (čija veličina varira) je često nejasan prikaz sadržaja te se koriste gumbi nejasnih naziva. Dodatno, današnja tehnologija često iziskuje čitanje korisničkih uputa, koje su uglavnom pisane vrlo sitnim tekstom i visoko stručnim jezikom.

Potrebe starijih korisnika isprepliću se s potrebama osoba s invaliditetom. Web stranice i ICT usluge s implementiranim opcijama pristupačnosti od koristi su kako osobama s invaliditetom/složenim komunikacijskim potrebama, tako i starijim korisnicima.

#### **11.4. Projekti koje se bave problematikom pristupačnost tehnologije korisnicima starije dobi**

*AGE Platforma Europa*<sup>37</sup> je europska mreža koja sadrži više od 150 organizacija osoba starije dobi i organizacija koje se bave osobama starijim od 50 godina, što predstavlja preko 40 milijuna starijih ljudi u Europi. Usmjerena je na širok spektar područja politike koja utječu na starije i umirovljenike: antidiskriminacija, zapošljavanje starijih radnika i aktivno starenje, socijalna zaštita, reforme mirovina, socijalna uključenosti, zdravlje, zlostavljanje starijih, međugeneracijska solidarnost, istraživanja, pristupačnost javnog prijevoza i nove tehnologije

---

<sup>37</sup> *Age Platform Europe*, <http://age-platform.eu/>

(ICT). AGE Platforma Europa vodi i aktivno sudjeluje u nekoliko projekata EU. Vezano uz pristupačnost i nove tehnologije, u okviru projekta se nalaze linkovi na aplikacije koje upućuju korisnike na fizičke lokacije na kojima je osigurana pristupačnost prilaza teško pokretnim osobama.

Projekt *Home Sweet Home*<sup>38</sup> ima za cilj razvoj usluga koje produljuju samostalan život starijih osoba u njihovom kućnom ambijentu, poboljšanje njihovog osjećaj sigurnosti i predlaže digitalne načine za poboljšanje njihove socijalne uključenosti. ICT rješenja usmjerena su integraciji senzora (praćenje pokreta, temperature prostorija, dima i sl.) s aplikacijama koje prate zdravstveno stanje starijih osoba (tlak, tjelesna težina, puls, šećer u krvi) te pomažu u efikasnom obavljanju svakodnevnih aktivnosti (aplikacije za vježbanje pamćenja, dnevni planer aktivnosti i sl.). Na temelju istraživanja provedenih u okviru projekta definirane su preporuke koje se tiču tehnoloških inovacija vezanih uz korisnike starije dobi:

- Rješenja se trebaju moći prilagoditi potrebama, očekivanjima, načinu života, sklonosti i rutini pojedinca.
- Treba uzeti u obzir kako i gdje stariji ljudi žive kako bi se izbjegao razvoj rješenja koja se ne mogu koristiti u stvarnim situacijama.
- Provjeriti pouzdanost rješenja prije nego što ih korisnici počnu upotrebljavati.
- Rješenja trebaju biti robustna, atraktivna i praktična, uzimajući u obzir odredbe energije i izazove vezane uz životni ciklus baterijskog napajanja.
- Koristiti *mainstream* tehnologije i rješenja integrirati - koliko je to moguće - na jednom uređaju.
- Pristupačnost treba biti u središtu tehnoloških inovacija za starije osobe.

*European Innovation Partnership on Active and Healthy Ageing*<sup>39</sup> (EIP AHA) u okviru svoje akcije *D4 Innovation for Age-friendly buildings, cities & environments* okuplja regionalne i lokalne vlasti u EU s dva osnovna cilja: produljenje od dvije zdrave godine života osobama starije dobi u EU ubrzanom promidžbom i implementacijom fizičkih i socijalnih okružja za podršku aktivnom i zdravom starenju te održavanje većeg sudjelovanja starijih građana, privatnih i javnih dionika i međusektorske suradnje u osmišljavanju i implementaciji inovacija i ICT rješenja prikladnih za osobe starije dobi. Jedno od područja u okviru ove akcije poduzima zajedničke inicijative za realizaciju učinkovitih inovativnih rješenja zasnovanih na ICT proizvodima, aplikacijama i uslugama u svrhu ostvarivanja životnog okružja prilagođenog starijim osobama.

---

<sup>38</sup> *Home Sweet Home*, <http://www.homesweethome-project.be/>

<sup>39</sup> *European Innovation Partnership on Active and Healthy Ageing*, [http://ec.europa.eu/research/innovation-union/index\\_en.cfm?section=active-healthy-ageing](http://ec.europa.eu/research/innovation-union/index_en.cfm?section=active-healthy-ageing)

Projekt *MyLife*<sup>40</sup> ima za cilj podržati neovisnost starijih osoba sa smanjenim kognitivnim funkcijama kao što su blago kognitivno oštećenje ili demencije korištenjem web usluga za snalaženje u vremenu, komunikaciju i zabavu.

Projekt FEARLESS<sup>41</sup> koristi potencijale i mogućnosti senzora u kombinaciji s akustičkim prepoznavanjem događaja. Vjeruje se da ova kombinacija može značajno poboljšati pouzdanost cjelokupnog sustava. pri detektiranju rizičnih situacija poput pojave dima, požara, poplave ili nagle promjene stanja osobe starije dobi prouzročene pogoršanjem zdravstvenog stanja.

Projekt The ENTRANCE<sup>42</sup> predstavlja europsku AAL (*Ambient Assisted Living*) inicijativu koja, među ostalim, predlaže ozbiljnu igru koja se koristi od strane osoba starije dobi kako bi poboljšali svoju prostornu kompetencije i, kasnije, njihova sposobnost za snalaženje i kretanje u zatvorenom i otvorenom prostoru. Mobilna platforma obuhvaća navigacijski softver koji se koristi za treninge na računalu te koji je također instaliran i pametni telefon te spojen s haptic navigacijskim uređajem (npr. narukvicom) za davanje uputa i informativnim poruka tijekom kretanja.

Ključni koncept projekta GoldUI<sup>43</sup> je razvoj i održavanje sigurnog korisničkog profila u oblaku, koji je namijenjen članovima obitelji ili stručnjaku koji skrbe o osobi starije dobi. Profil sadrži podatke o preferencijama korisnika, stanju vida i sluha, mobilnosti, memorijskim mogućnostima i postavke komunikacije, kao i podatke o računu za ključne usluge putem niza dodataka. Ključne tehnološke inovacije koje se žele uvesti su prikaz opisa višemedijskog zapisa, personalizacija i kontekstualizacija informacija, interaktivna pretraga i klijentska korisnička sučelja za prirodniju interakciju i pojednostavljenje složenih zadataka te povećanje znanja korisnika starije dobi.

### **11.5. Pristupačnost web sjedišta**

Web pristupačnost je praksa u web dizajnu kojom se svim korisnicima nastoji omogućiti pristup i korištenje sadržaja na webu. Kako bi web sjedište bilo pristupačno, moraju se ukloniti barijere s kojima se susreću skupine korisnika s različitim poteškoćama (vida, sluha, motorike, kognitivnim i sl.).

Korisnicima s oštećenjima vida koji koriste čitače ekrana (*screen reader*) olakšan je pristup ako za sve slike postoje odgovarajući tekstualni opisi. Slabovidni korisnici lakše će čitati sadržaj ako im je ponuđena opcija povećanja veličine fonta. Korisnici s teškoćama prepoznavanja boja lakše će se snaći na web sjedištu na kojem su boje i oznake odabrane tako

---

<sup>40</sup> *MyLife*, <http://www.mylife-project.org>

<sup>41</sup> FEARLESS, <http://www.aal-europe.eu/projects/fearless/>

<sup>42</sup> The ENTRANCE, <http://www.aal-europe.eu/projects/entrance>

<sup>43</sup> GoldUI, <http://www.goldui.eu>



da se elementi stranice jasno razlikuju. Web sjedišta dizajnirana tako da se njima može efikasno kretati samo tipkovnicom ili nekom drugom tehnologijom za pristupačnost olakšava korištenje skupini korisnika s poteškoćama s motorikom ruku. Jasno pisan i dobro ilustriran sadržaj olakšava korištenje web sjedišta osobama s poteškoćama u učenju.

Povećanjem broja sjedišta weba koja implementiraju načela web pristupačnosti, sve više korisnika može lakše koristiti i doprinosti web sadržajima. Ako je web sjedište pristupačno, korištenje i pristupanje sadržaju vjerojatno će biti olakšano svim skupinama korisnika bez obzira na invaliditet ili dob.

Postoje brojna istraživanja vezana uz analizu pristupačnosti web sjedišta. Većina istraživanja zaključuje da se potrebe osoba s invaliditetom uvelike preklapaju s potrebama osoba starije dobi koji imaju funkcijska ograničenja povezana s dobi. Dio istraživanja zaključuje da je ono što je korisno i prilagodljivo osobama starije dobi zapravo kvalitetan dizajn koji je pogodan za korištenje i ostalim korisnicima [6]: konzistentna navigacija, razumljiv i strukturirani sadržaj i sl. Navedena studija također naglašava činjenicu da su starije osobe vrlo nehomogena skupina korisnika čije mogućnosti i potrebe znatno variraju od pojedinca do pojedinca, a poteškoće u primjeni ICT rješenja su višestruke i mogu biti grupirane na različite načine. Navedena činjenica zahtijeva da se u postojeća i nova ICT rješenja ugrade različite mogućnosti prilagodbe, kako prikaza tako i samog sadržaja [13].

#### **11.6. Smjernice i preporuke za osiguranje pristupačnosti usluga weba**

Usluge weba su važan resurs u mnogim aspektima života: obrazovanju, zapošljavanju, upravljanju državom, trgovini, zdravstvu, rekreaciji, pristupu informacijama i komunikaciji. Sve usluge weba, posebno one koje su od javnog interesa, trebaju imati osiguran jednaki pristup i jednake mogućnosti za osobe s invaliditetom i osobe starije dobi.

Istraživanje [4] upućuje na četiri najčešća aspekta na koje treba obratiti pozornost pri dizajnu usluga weba koji su prikazani u Tablici 3.1.

Smjernice za osiguravanje pristupačnosti mrežnog sadržaja upozoravaju na navedene probleme s kojima se susreću osobe s invaliditetom i osobe starije dobi te sadrže preporuke kako učiniti sadržaj pristupačnijim. Dobrim razumijevanjem i ispravnom implementacijom smjernica, web dizajneri mogu značajno poboljšati pristupačnost svoje stranice i učiniti da njihov sadržaj mogu konzumirati svi korisnici ravnopravno.

**Tablica 3.1.** Najčešći aspekti na koje treba obratiti pozornost pri dizajnu usluga weba

A1. Dizajn interakcija	A2. Informacijska arhitektura	A3. Vizualni dizajn
<ul style="list-style-type: none"> <li>- Slijediti uobičajene konvencije pri izradi dizajna (npr. podcrtani linkovi)</li> <li>- Pomicanje miša za kretanje po korisničkom sučelju je naučeno ponašanja i s vremenom korisnicima starije dobi postaje otežano korištenje sljedećih elemenata: pull-down menus, scrolling lists, scrolling pages. U dizajn ugraditi alternativne opcije.</li> <li>-Prepoznavanje i pristupanje elementima sučelja na koje se može kliknuti često je otežano - dizajnom naglasiti takve elemente</li> <li>- Povratna informacija nakon korisničke akcije (vizualna, auditivna) je korisno pomagalo za lakše razumijevanje i korištenje elemenata korisničkog sučelja.</li> </ul>	<ul style="list-style-type: none"> <li>- Opisuje informacijsku strukturu sjedišta weba i način na koji će se korisnici kretati sjedištem</li> <li>- Jasno označavanje (linkova, naslova i stavki izbornika)</li> <li>- Jednostavan i konzistentan tekst</li> <li>- Širina vs. dubina - informacije organizirati u što manje hijerarhijskih nivoa za lakše snalaženje stariji osoba</li> <li>- Redundantni linkovi - omogućavanje dolaska do informacije iz više smjerova</li> </ul>	<ul style="list-style-type: none"> <li>- Stariji korisnici s iskustvom u korištenju ICT rješenja pregledavaju sadržaje na isti način kao i mlađi korisnici, dok starijim korisnicima s manje iskustva irelevantne informacije koje se pojavljuju na korisničkom sučelju (poput reklama) otežavaju pregledavanje sadržaja</li> <li>- Treba postojati mogućnost prilagodbe veličine teksta i kontrasta pozadine i teksta, uključujući naslove</li> </ul>

### 11.6.1. Smjernice WCAG

WCAG 2.0 (*Web Content Accessibility Guidelines*) smjernice usvojene su 2008. godine od strane inicijative *Web Accessibility Initiative* (WAI). Navedena Inicijativa za pristupačnost Interneta radi unutar W3C-a (*World Wide Web Consortium*), međunarodne udruge koja se bavi razvojem i standardizacijom weba.

Postojeće smjernice za pristupačnost weba nude rješenja za poboljšanje pristupačnosti potrebe starijih korisnika weba. Smjernice WCAG podijeljene su na tri razine po prioritetima. Smjernice prve razine (A) *moraju* se koristiti u oblikovanju web sadržaja, smjernice druge razine (AA) *trebale* bi se koristiti, a smjernice treće razine je *preporučljivo* koristiti (AAA).

Prije smjernica WCAG 2.0, na snazi su bile smjernice WCAG 1.0 objavljene 1998. godine. Navedene smjernice razlikuju se u širini tehnologija na koje se odnose te određivanju usklađenosti s web sadržajem. Dok se prethodna verzija smjernica odnosi na HTML i CSS, smjernice WCAG 2.0 su predložene na način da se mogu primijeniti na postojeće i buduće tehnologije bez obzira na to jesu li razvijene unutar W3C-a ili van njega (JavaScript, Flash, PDF, i slično).

Smjernice WCAG 2.0 počivaju na četiri načela za pristup i korištenje web sadržaja. Svako načelo sadrži određeni broj smjernica te svaka od tih smjernica ima kriterij uspješnosti koji može odgovarati razini A, AA ili AAA. Izostavljanjem bilo kojeg načela, pristup sadržaju bi nekoj skupini korisnika bio onemogućen. Ukupno postoji 12 smjernica koje su tehničke naravi i zahtijevaju dobro poznavanje tehnologija weba za razumijevanje i primjenu. Smjernice se implementiraju u kasnim fazama razvoja sjedišta weba s ciljem odgovora na probleme pristupačnosti koji su identificirani u studijama upotrebljivosti weba [3].

## Načela web pristupačnosti prema smjernicama WCAG

- **Vidljivost**

Elementi korisničkog sučelja i sadržaj web stranica/sjedišta trebaju biti dostupni korisnicima na način na koji ih oni mogu opaziti. Ako sadržaj nije dostupan putem barem jednog osjetila, tada nije pristupačan. Iako je ovo načelo samo po sebi očigledno, u praksi se često ignorira te postoji veliki broj stranica sadrži informacije koje nisu pristupačne određenoj skupini korisnika. Treba omogućiti pojavu informacije u različitim oblicima, kako bi se mogla opaziti na različite načine što se postiže odvajanjem sadržaja od prikaza. Iako je cilj prezentacije obogatiti sadržaj kako bi korisničko iskustvo bilo potpunije, informacije ne smiju ovisiti o prezentaciji.

- **Operabilnost**

Linkovi, navigacija, različite opcije koje nudi stranica moraju biti implementirani na način da su dostupni korisniku bez obzira na to koristi li miša, tipkovnicu ili neki uređaj iz kategorije asistivne tehnologije. Sadržaj kojemu se može pristupiti samo putem miša neće biti pristupačan osobi koja ne može koristiti standardni miš. To može biti zbog tremora, nedovoljne kontrole pokreta ili invaliditeta. U tom slučaju, osoba je primorana koristiti razne pomoćne uređaje i/ili tipkovnicu. Asistivne ulazne jedinice su od velike pomoći osobama koje su slabovidne ili slijepe.

Preporučljivo je da korisnici nisu vremenski ograničeni kako bi izvršili određene aktivnosti ili radnje na webu u situacijama kad se ne ugrožava sigurnost korisnika. Također, potrebno je implementirati opciju oporavka od neispravno poduzete akcije korisnika (dodatna provjera želi li doista korisnik poduzeti određenu akciju pojavom prozora za potvrdu, upozorenja, ali i uputa ako je sadržaj kompliciran ili ako je nalaženje informacija otežano).

- **Razumljivost**

Ako je osigurana vidljivost i operabilnost, ali sadržaj je nerazumljiv, stranica nije pristupačna. Dobra praksa je osigurati alternativne informacije koje poboljšavaju razumljivost sadržaja (pojašnjenje teksta ilustracijama/audio zapisom). Takve dodatne informacije su ponekad od izuzetne važnosti osobama s kognitivnim poteškoćama i poteškoćama u čitanju.

- **Robusnost**

Ovo načelo zahtijeva sposobnost web stranice da je tumači širok spektar korisničkih agenata (web preglednici, programi za reprodukciju glazbe i filmova, dodaci te pristupačne tehnologije poput povećala za ekran ).

Za efikasnu prilagodbu usluga weba starijim osobama WAI preporučuje implementaciju barem svih WCAG 2.0 razina A i AA.

Pri implementaciji smjernica WCAG 2.0, programeri mogu koristiti različite tehnike kako bi se zadovoljili kriterije uspješnosti. U nekim slučajevima, korištenje jedne tehnike umjesto

druge može optimizirati pristupačnosti za određene korisnike. Ovo poglavlje navodi neke od tehnika koje mogu pomoći optimizirati web stranice za starije osobe.

Inicijativa WAI je uz preporuke objavila i primjere kako dizajnirati ICT usluge koje su prilagođene osobama starije dobi<sup>44</sup>.

Za osobe s težim oštećenjima vida preporuča se korištenje čitača ekrana (*screen reader*) u kombinaciji s opcijama povećanja veličine fonta teksta te kontrasta kako bi stranicu učinile što čitljivijom.

Osobe s motoričkim teškoćama umjesto miša mogu koristiti tipkovnicu ili neku drugu tehnologiju za pristupačnost. Sjedišta weba dizajnirana tako da se njima može efikasno kretati samo tipkovnicom ili drugom tehnologijom olakšava starijim osobama pristup web sadržaju.

Osobe s oštećenjem sluha trebale bi biti u mogućnosti vidjeti tekstualnu ili ilustrativnu reprezentaciju bilo kakvog audio sadržaja koji je dio web stranice.

Osobe s kognitivnim poteškoćama zahtijevaju što jednostavniji tekst i primjereni izgled web sadržaja te je kod njih osobito važna dosljedna navigacija i prezentacija.

U Tablici 3.2. su navedene preporuke vezane dizajn web sjedišta kojima se ona mogu učiniti pristupačnima osobama starije dobi nastala na temelju analize literature [3][7][8][9][10][13]

**Tablica 3.2.** Preporuke vezane uz dizajn pristupačnog sjedišta web za osobe starije dobi

Oblikovanje teksta	Odjeljci teksta poravnavaju se na lijevu stranu te se međusobno odvajaju razmacima.
	Kako bi stranica izgledala što jasnije, preporučuje se korištenje samo jednog stila teksta te izbjegavanje kosih slova ( <i>italic</i> ).
	Preporučuje se korištenje stila ( <i>font</i> ) „Arial“, uz veličinu teksta 12 ili 14 te mogućnost dodatnog povećanja umetanjem gumba za povećanje ( <i>button</i> ) na vrhu stranice.
	Tekst se treba moći povećati do do 200 posto bez ikakvih gubitka sadržaja ili funkcionalnosti.
	Predlaže se izbjegavanje korištenja samo velikih ili samo malih slova kako bi se stranica izgledala jednostavnije, a dodatno se može i bojama vizualno grupirati informacije.
	Korištenje pozadina bez uzoraka i kontrasta između teksta i pozadine barem 4.5:1. Kontrast predstavlja omjer najsvjetlije i najtamnije boje te se mijenja ovisno o veličini teksta.
	Preporučuje se korištenje kontrasta najmanje 4.5:1 kod normalnog teksta, odnosno 7:1 kod uvećanog teksta [10].
	Također, stranica bi trebala imati ugrađeni opciju za mijenjanje kontrasta

<sup>44</sup> *How WCAG 2.0 Applies to Older People*, <http://www.w3.org/WAI/older-users/developing.html#map>

	<p>ovisno o potrebama korisnika [9].</p>
Dosljedna organizacija web stranice	<p>Stranica treba biti organizirana na predvidljiv i dosljedan način kako bi korisnici se korisnici što lakše snalazili.</p>
	<p>Elemente koji na isti način funkcioniraju i povezane teme preporučljivo je organizirati konzistentno [10].</p>
	<p>Elementi bi trebali biti jasno vidljivi, istog oblika kroz cijelu stranicu te je poželjan razmak između njih kako bi se ostavio veći prostor za točan odabir pojedinog elementa.</p>
	<p>Važno je korisnika fokusirati na bitne elemente stranice, a korisnici se lakše snalaze ako su informacije hijerarhijski navedene prema značaju [7].</p>
Jednostavno kretanje po web stranici	<p>Omogućiti što jednostavnije i efikasnije kretanje po sjedištu weba</p>
	<p>Ugraditi navigaciju korak po korak, omogućiti povratak na glavnu stranicu na svim ostalim mjestima unutar sjedišta weba.</p>
	<p>Poželjno je ugraditi opciju pretraživanja stranice (<i>search box</i>) kako bi što lakše pronašli pojedini elementi, a dodatno je moguće olakšati pretraživanje umetanjem alternativne riječi za krivo unesenu.</p>
	<p>Da bi se izbjeglo nekontrolirano kretanje po stranici izbjegava se automatsko pomicanje teksta (<i>scrolling</i>) i ne stavlja se horizontalno kretanje, već se upotrebljava vertikalno pomicanje koje je jednostavnije [10].</p>
Izbornici ( <i>menus</i> ), gumbi ( <i>buttons</i> ) i kućice ( <i>boxes</i> )	<p>Pravilnom organizacijom izbornika, pospješuje se snalaženje na stranici i njeno efikasno korištenje.</p>
	<p>Izbornici se trebaju otvarati i zatvarati klikom miša, a svaka stavka izbornika treba biti jasno definirana.</p>
	<p>Kraj polja za unos, uvijek s iste strane i u istu liniju, potrebno je staviti labelu.</p>
	<p>Važno je tekstem opisati kućice, kako bi korisniku prilikom svake interakcije bilo jasno što treba učiniti.</p>
	<p>Također, korisniku se može ponuditi alternativna opcija, ako ne želi odabrati predloženu.</p>
	<p>U nekim situacijama dobro je ponuditi mogućnost ispravljanja određene akcije ili otkazivanja iste [AP2].</p>
	<p>Na vrhu određenih obrazaca treba objasniti koja su polja za unos obavezna te ih opisati crvenim tekstom i nekim simbolom, najčešće zvjezdicom (" * ") [AP3].</p>
Poveznica (link)	<p>Za opisivanje poveznica nije poželjno koristiti skraćenice, već se preporučuje potpuni opis koji počinje jedinstvenom ključnom riječi.</p>
	<p>Stranica ne bi smjela imati puno poveznica jer to pridonosi konfuznosti prilikom korištenja.</p>
	<p>Preporučljivo je ugraditi mehanizme koji prelaskom preko poveznice mijenjaju njenu boju te ju stavljaju u fokus.</p>
	<p>Olakšati korištenje poveznica može ignoriranje drugog klika miša, kako bi se izbjeglo neželjeno skakanje sa stranice na stranicu [10].</p>
Dodatne smjernice za efikasnije korištenje web stranica starijim osobama	<p>Starijim osobama može se olakšati korištenje web stranica zabranom različitih elemenata koji se kreću po ekranu ili trepću.</p>
	<p>Zvukove treba uključiti samo na zahtjev korisnika te mu se omogućuje odgađanje nekih vremenskih ograničenja.</p>
	<p>Prije otvaranja novog prozora, korisnika treba upozoriti kako bi bio spreman na promjenu konteksta.</p>
	<p>Pomoć prilikom pregledavanja web stranice moguća je u obliku uputa koje jasno definiraju što treba sljedeće učiniti.</p>
	<p>Ako dođe do pogreške, mora postojati mogućnost za povratak i oporavak od pogreške, a dodatno se može korisniku omogućiti pregledavanje pogreški do kojih je došlo.</p>

#### 11.6.2. ITU preporuka: F.790 (01/07) Telecommunications accessibility guidelines for older persons and persons with disabilities

Preporuke imaju za cilj pružiti opće smjernice za standardizaciju, planiranje, razvoj, projektiranje i distribuciju svih oblika telekomunikacijske opreme i softvera i povezanih telekomunikacijskih usluga kako bi se osigurala njihova dostupnost korisnicima s najrazličitijim rasponom sposobnosti/posebnih potreba. Preporuke osiguravaju smjernice za razumijevanje problema pristupačnosti i implementacija opcija koje osiguravaju pristupačnost u proizvode i usluge.

#### 11.6.3. Smjernice pristupačnosti prema članku 508 (Section 508 Accessibility Guidelines)<sup>45</sup>

Od ukupno 16 smjernica, 11 njih se zasniva na smjernicama WAI. Sadrže jednostavniji skup zahtjeva koje treba implementirati u sjedišta weba pri čemu nije potrebno radikalno promijeniti strukturu web stranice osim značajni promijeniti korištenje dinamičkog HTML-a i tehnologije Flash.

#### 11.6.4. Najbolje prakse/preporuke Googla za implementaciju pristupačnosti namijenjene Android razvijateljima<sup>46</sup>

Pokretni uređaji s instaliranim operacijskim sustavom Android ovisno o svojim tehnološkim značajkama nude različite mogućnosti za pristupačnost poput pretvaranja teksta u govor (na engleskom jeziku), haptičke povratne veze, korištenje navigacije gestama, trackball miša kao i kontrole s tipkama za svaki smjer (directional pad, d-pad) . Osnovne preporuke programerima tiču se povratne audio informacije, korištenja alternativnih načina navigacije te fizičke povratne informacije. Definirane su razvojni prakse i značajke programskih sučelja(API) za osiguranje pristupačnosti, kontrolna lista za provjeru jesu li aplikacije pristupačne te preporuke kako koristiti značajke programskih sučelja (API) za razvoj posebnih aplikacija koje čine pristupačnim postojeće aplikacije.

### **11.7. Korisnička sučelja novih generacija pokretnih uređaja i korisnici starije dobi**

Tehnologija je uvijek jedan korak ispred i dok se još nisu riješili problemi pristupačnosti na starijim uređajima poput stolnih računala, pojavili su se novi uređaji koji su osobama s invaliditetom i osobama starije dobi donijeli nove izazove, ali i nove potencijale za ICT rješenja koja im mogu poboljšati kvalitetu života ako se ispravno implementiraju.

U domeni razvoja pokretnih uređaja poput pametnih telefona i tableta ne postoji odgovarajući skup standardiziranih i široko primjenjivanih smjernica s naglaskom pristupačnost. Pojedinačni napor u tom području predstavlja istraživanje [11] koje predlaže smjernice za postizanje pristupačnosti namijenjeno pokretnim korisničkim sučeljima temeljen na literaturi, postojećim standardima i najboljim praksama.

---

<sup>45</sup> *Section508.gov, Opening Doors to IT*, <http://www.section508.gov/>

<sup>46</sup> Android Developers, *Accessibility*, <https://developer.android.com/guide/topics/ui/accessibility/index.html>

### 11.7.1. Mobilne aplikacije za starije korisnike

Analizom postojećih lista <sup>474849505152</sup> s najčešćim preporučenim aplikacijama od strane samih korisnika starije dobi za oba operacijska sustava (Android i iOS) te za pametne telefone i tablet uređaje, mogu se definirati kategorije mobilnih aplikacija i njihove osnovne funkcionalnosti koje osiguravaju pristupačnost illi pomažu korisnicima u praćenju zdravstvenog stanja te održavanju kognitivnih mogućnosti.

#### **Aplikacije vezane uz zdravlje**

- Aplikacije za bilježenje visine krvnog tlaka, otkucaja srca i tjelesne težine te praćenje u vremenu
- Podsjetnici/alarmi za uzimanje lijekova
- Pohranjivanje/arhiviranje medicinske dokumentacije u digitalnom obliku na uređaju
- Aplikacije za vježbanje pamćenja i poboljšanje kognitivnih vještina
- Kognitivni testovi za demenciju
- Komunikacijsko pomagalo zasnovano na fotografijama za osobe s demencijom
- Test za gerijatrijsku depresiju
- Aplikacija za podršku fizioterapiji

#### **Aplikacije s funkcijom asistivnih tehnologija**

- Pokretni uređaj kao povećalo za čitanje teksta koji se nalazi ispred njega (s uključenom bljeskalicom)
- Povećani prikaz kontakata u imeniku na uređaju
- Aplikacija koja povećava navigacijske tipke
- Aplikacije koje čitaju elektroničku poštu, tekstualne datoteke i web sadržaj

---

<sup>47</sup> Official SeniorNet Headquarters Blog, *Social Media Scoop for Senior*, <http://seniornet.org/blog/16-helpful-apps-for-seniors/>

<sup>48</sup> Tabtimes, *10 Great Tablet Apps for Seniors*, <http://tabtimes.com/slideshow/ittech-apps/2014/07/16/10-great-tablet-apps-seniors>

<sup>49</sup> *Best free smartphone and tablet apps for older people*, <http://www.geeksquad.co.uk/articles/best-free-smartphone-and-tablet-apps-for-older-people>

<sup>50</sup> *Androids for Seniors*, <http://www.androids4seniors.com/>

<sup>51</sup> Appyie, *5 of the Best Apps for Older People*, <http://appyie.com/5-of-the-best-apps-for-older-people/>

<sup>52</sup> MyAgeingParent, *Top apps for the elderly*, <http://www.myageingparent.com/top-ipad-apps-for-the-elderly/>

- Prilagodba sučelja pokretnog uređaja s povećanim ikonama, interaktivnom pomoći za svaku ikonu koja se pojavljuje na ekranu, implementirane opcije slanja SOS poruke i prikazivanje trenutne lokacije

### Aplikacije za pomoć u obavljanju svakodnevnih aktivnosti

- Detektor pada
- Memoriranje parkirnog mjesta automobila u garaži putem jednostavnog sučelja i alarm za istjecanje parkirne karte
- Financijske aplikacije za bilježenje prihoda i rashoda te predlaganje preraspodjela financijskih sredstava u svrhu štednje
- Aplikacije za uspavlivanje s različitim zvučnim pozadinama

### 11.8. Alati za provjeru e-pristupačnosti sjedišta weba

Alati za provjeru pristupačnosti su programska rješenja ili web usluge koji evaluiraju ispunjava li određeni sadržaj na web stranici smjernice o dostupnosti. Ovi alati značajno smanjuju vrijeme i napore za procjenu web stranice, a temeljem dobivenih rezultata evaluacije mogu se ugraditi u web stranicu određena poboljšanja s ciljem poboljšanja pristupačnosti.

Lista koja se nalazi na stranicama inicijative W3C WAI<sup>53</sup> nastala je objavama pojedinih davatelja usluge on-line evaluacije te može poslužiti kao koristan repozitorij alata. Neki od alata iz te liste prikazani su u Tablici 3.3.

**Tablica 3.3.** Primjeri alata za provjeru pristupačnosti prema listi inicijative W3C WAI

<p><b>Achecker</b></p> <p><a href="http://achecker.ca/checker/index.php">http://achecker.ca/checker/index.php</a></p> <p>(The Adaptive Technology Resource Centre (ATRC) at the University of Toronto)</p>	<p>- Evaluacija HTML sadržaja s ciljem detekcije problema pristupačnosti</p> <p>- Analiza prema smjernicama WCAG 1.0 (International), WCAG 2.0 (International), BITV 1.0 (Germany), Section 508 (U.S.), Stanca Act (Italy)</p> <p>Licenca: <i>Open source SW</i></p> <p>- Input: URL web sjedišta, učitavanje HTML datoteke, ili kopiranje HTML izvornog koda web stranice</p>	<p><b>Struktura izvještaja:</b></p> <p>- smjernica koju određena linija koda ne zadovoljava</p> <p>- razlog zašto je došlo do kolizije s odredbom smjernice</p> <p>- broj linija gdje je došlo do kolizije</p> <p>- opis prijedlog za rješenje problema (tekstualni i u formi programskog koda)</p> <p><b>Format izvještaja:</b></p> <p>EARL<sup>54</sup> (XML-based Evaluation and Report Language)</p>
--	--	--

<sup>53</sup> *Web Accessibility Evaluation Tools* List, <http://www.w3.org/WAI/ER/tools/>, zadnji pristup 24.11.2014.

<sup>54</sup> EARL je format koji je razvijen za prikaz i interpretaciju rezultata testiranja provedenih na sjedištima i stranicama weba. Najveću primjenu ima u razvoju tehnologija za web pristupačnost i kontrolu web sadržaja gdje se koristi za opis i klasifikaciju sadržaja.



<p><b>A-Tester</b>  <a href="http://www.evaluera.co.uk/">http://www.evaluera.co.uk/</a>                  (Evaluera Ltd, Velika Britanija)</p>	<p>Alat uspoređuje početni dizajn web stranice s konačnim dizajnom koji ima implementirano progresivno poboljšanje u skladu sa zadanim smjericama<sup>55</sup> (<i>Online checker</i>)</p> <p>Licenca: <i>Free</i></p> <p>Input: pojedinačne web stranice, stranice s pristupom zaštićenim lozinkom.</p> <p>Preglednik: Chrome</p>	<p><b>Tehnologije:</b> HTML, HTML5  <b>Format izvještaja:</b> HTML</p>
<p><b>Functional Accessibility Evaluator 2.0 beta</b>  <a href="http://fae20.cita.illinois.edu/">http://fae20.cita.illinois.edu/</a>                  (University of Illinois)</p>	<p>Evaluiira sjedišta weba s obzirom na smjernice WCAG 2.0 Level A and AA. Assists with: Generating reports of evaluation results (<i>Online checker</i>)</p> <p>Input: Skup web stranica ili web sjedište</p> <p>API: Web servis (Rest API, Webhook...)</p> <p>Licenca: <i>Open Source</i></p>	<p><b>Tehnologije:</b> CSS, HTML, XHTML  <b>Struktura izvještaja:</b> Sažetak i detaljni izvještaj  <b>Format izvještaja:</b> HTML, XML</p>
<p>WCAG Compliance Auditor  <a href="http://www.funnelback.com/our-products/wcag-compliance-auditor">http://www.funnelback.com/our-products/wcag-compliance-auditor</a>                  (Funnelback, Australija)</p>	<p>Alat identificira pogreške vezane uz pristupačnost, daje preporuke kako ih ispraviti popraviti i predlaže metriku za mjerenje pristupačnosti tijekom vremena (<i>Hosted service, Server installation</i>).</p> <p>Input: pojedinačne web stranice, grupe stranice, sjedište weba ili grupe sjedišta, stranice s ograničenim pristupom, stranice zaštićene lozinkom</p> <p>APIs: Java, Web service (Rest API, Webhook...)</p> <p>Licenca: <i>Commercial</i></p>	<p><b>Tehnologije:</b> HTML, XHTML, PDF  <b>Format izvještaja:</b> HTML, PDF, CSV</p>
<p>WAVE  <a href="http://wave.webaim.org/">http://wave.webaim.org/</a>                  (WebAIM, Utah State University, SAD)</p>	<p>Skupina alata za evaluaciju pristupačnosti vizualnim prikazom problema pristupačnosti na nekoj stranici. (<i>Online checker, Hosted service, Server installation</i>)</p> <p>API: Web service (Rest API, Webhook...)</p> <p>Licenca: Free Software, Trial or Demo, Commercial</p>	<p><b>Tehnologije:</b> CSS, HTML, XHTML, Images  <b>Format izvještaja:</b> HTML, XML  <b>Struktura izvještaja:</b>                  - Izvještaj s rezultatima analize                  - Prikaz informacija unutar web stranice                  - Promjena prikaza web stranice</p>
<p>W3C mobileOK Checker  <a href="http://validator.w3.org/mobile/">http://validator.w3.org/mobile/</a> (W3C)</p>	<p>Alat služi za provjeru mobilne pristupačnosti web dokumenata. Koristi Java Library koji provjerava HTML kod stranice koja mu je zadana.</p>	<p>Alat vraća popis svih grešaka u obliku tablice na novoj web stranici. Rezultati testiranja ukazuju koje su najteže greške i kako ih popraviti.</p>

<sup>55</sup> WCAG 2.0 Level-AA conformance statements for HTML5 foundation markup

### 11.9. Analiza pristupačnosti najposjećenijih sjedišta web katoga [www.hr](http://www.hr)

Za analizu je korišten alat AChecker. Analizirano je 20 sjedišta weba koja su prema statistici službenog CARNetov kataloga [www](http://www) poslužitelja u Hrvatskoj<sup>56</sup> najposjećenija. Izuzete su sjedišta pornografskog i astrološkog sadržaja te su preostala sjedišta kategorizirana u sljedeće kategorije: Prodaja vozila, News portali, Institucije državne uprave i Putovanja (najposjećenija sjedišta weba turističkih agencija).

Alat AChecker u svojoj analizi može imati tri moguća rezultata:

- Problem - neimplementiranje određenih smjernica WAI tijekom dizajna stranice, alat je siguran da se radi o problemu s određenom sigurnošću)
- Najvjerovatniji problem - sigurnost kojom alat identificira ovaj problem zahtijeva analizu od strane čovjeka za donošenje konačne odluke je li doista potrebno napraviti promjenu)
- Potencijalni problem - alat ga ne može identificirati, potrebna analiza od strane čovjeka.

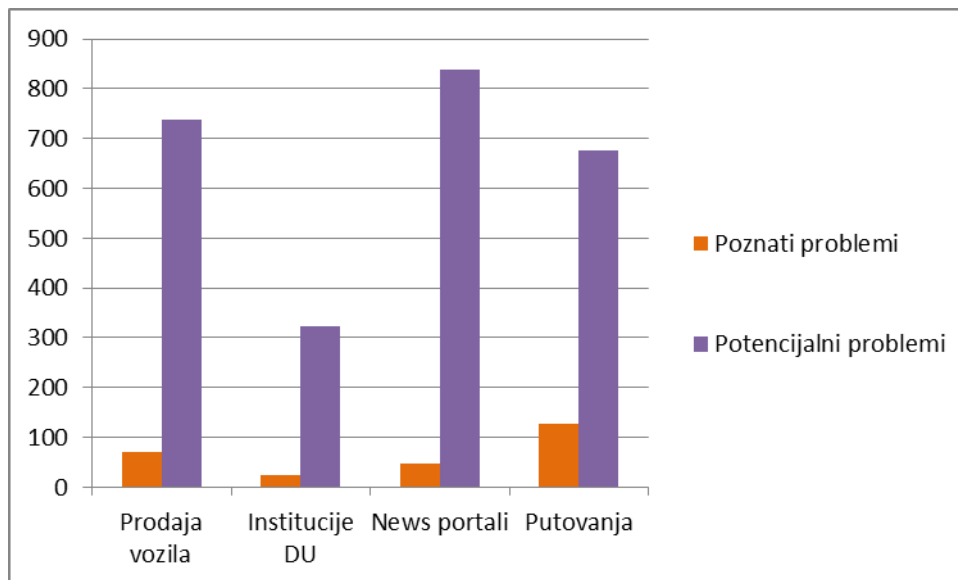
Uz sve tipove problema alat nudi opis iz kojega se može zaključiti kako problem treba riješiti. Primjeri problema koji su se pojavili tijekom analiza najposjećenijih sjedišta weba u okviru kataloga [www.hr](http://www.hr) nalaze su u Tablici 3.4.

**Tablica 3.4.** Primjeri opisa koji se pojavljuju uz određene probleme identificiranih alatom AChecker

Problemi	Text Alternatives: Provide text alternatives for any non-text content. Adaptable: Create content that can be presented in different ways (for example simpler layout) without losing information or structure. Navigable: Provide ways to help users navigate, find content, and determine where they are. Readable: Make text content readable and understandable. Distinguishable: Make it easier for users to see and hear content including separating foreground from background. Navigable: Provide ways to help users navigate, find content, and determine where they are. Compatible: Maximize compatibility with current and future user agents, including assistive technologies.
Najvjerovatniji problemi	Likely: Image Alt text may be too long. Select element may cause extreme change in context.
Potencijalni problemi	Text Alternatives: Provide text alternatives for any non-text content img element may require a long description. Distinguishable: Make it easier for users to see and hear content including separating foreground from background. Image may be using color alone. Navigable: Provide ways to help users navigate, find content, and determine where they are. Document may be missing a „skip to content“ „link“.

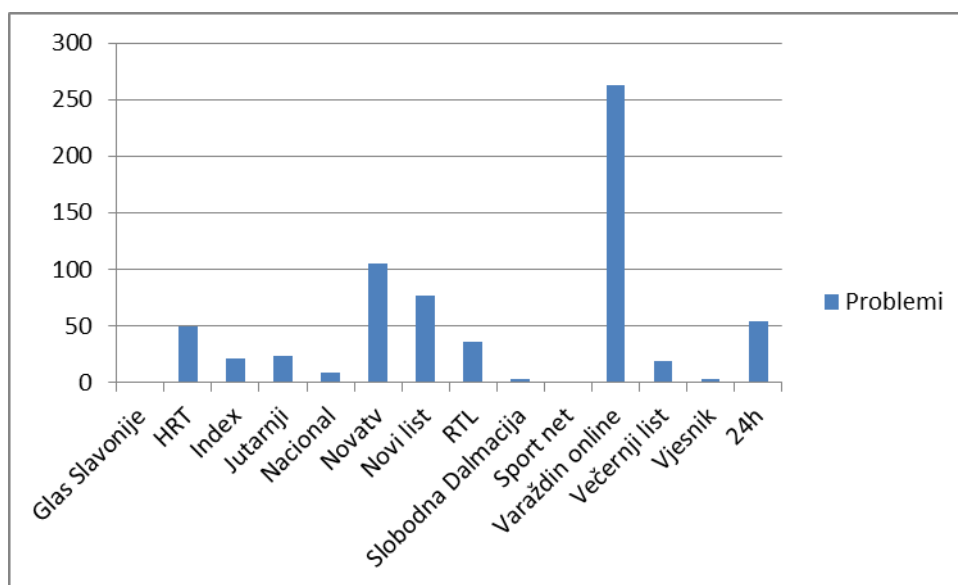
<sup>56</sup> WWW.HR - početna stranica Hrvatske, <http://www.hr>

Rezultati analize najposjećenijih stranica kataloga [www.hr](http://www.hr) u kategorijama prodaja vozila, institucije državne uprave, news portali i turističke agencije prikazani su na Slici 3.1. Može se zaključiti da se općenito sjedišta weba institucija državne uprave najprilagođenija osobama sa složenim komunikacijskim potrebama, dok su stranice komercijalnih djelatnosti i news portala s više potencijalnih barijera za pojedine kategorije korisnika.



**Slika 3.1.** Rezultati analize kategoriziranih najposjećenijih stranica kataloga [www.hr](http://www.hr)

Analiza najposjećenijih web sjedišta news portala prikazana je na Slici 3.2. Portali *Glasa Slavonije* i *Sport neta* nema niti jedan problem sa sigurnošću pronađen od korištenog alata za provjeru pristupačnosti, što znači da ga mogu koristiti sve kategorije korisnika. Ovo je izvrstan primjer društvene osviještenosti i angažiranosti i omogućavanja pristupa informacija svima!



**Slika 3.2.** Analiza pristupačnosti najposjećenijih news portala u okviru kataloga [www.hr](http://www.hr)

### 11.9.1. Provjera pristupačnosti web stranica na mobilnim uređajima

Za najposjećenija sjedišta weba kataloga [www.hr](http://www.hr) procijenjeno je koji su najposjećeniji od strane osoba starije dobi. Za ta sjedišta provjerena je pristupačnosti sjedišta weba na mobilnim uređajima s alatom mobileOK Checker. Rezultati su prikazani u Tablici 3.5. Diskusija rezultata s razvijateljima pojedinih analiziranih web sjedišta ukazuje da se kategoriziranje broj ugrađenih vanjskih resursa i veličina web stranice kao kritičnih neispravnosti smatra spornim zbog same naravi današnjih dinamičkih web sjedišta.

**Tablica 3.5.** Analiza pristupačnosti zadanih sjedišta weba na mobilnim uređajima

Projektno web sjedište za korisnike potpomognute komunikacije	0% prolaznosti - pronađeno 13 grešaka (5 kritičnih) previše ugrađenih vanjskih resursa te veličina web stranice detektiran pop-up prozor koji na malom ekranu može izazvati nečitljivost i konfuziju sintaksne greške u CSS-u zbog kojih neki preglednici neće biti u mogućnosti učitati stranicu. u headeru nije specificiran encoding zbog čega se neki znakovi možda neće ispravno prikazati. na nekim slikama nedostaju atributi visine i širine zbog čega neki preglednici moraju presložiti stranicu nakon što je učitana nisu sve slike u GIF/JPEG formatu zbog čega ih neki preglednici neće moći prikazati.
Web portal dnevnih novina	0% prolaznosti - pronađeno 11 grešaka (6 kritičnih) previše ugrađenih vanjskih resursa te veličina web stranice preglednici koji ne pridržavaju javascript neće moći prikazati sve elemente stranice detektiran pop-up prozor koji na malom ekranu može izazvati nečitljivost i konfuziju sintaksne greške u CSS-u zbog kojih neki preglednici neće biti u mogućnosti učitati stranicu. u headeru nije specificiran encoding zbog čega se neki znakovi možda neće ispravno prikazati. na nekim slikama nedostaju atributi visine i širine zbog čega neki preglednici moraju presložiti stranicu nakon što je učitana
Nezavisni informativni portal	63% prolaznosti - pronađeno 8 grešaka (1 kritična) korištenje javascripta nespecificiranje veličine slika korištenja nekih HTML elemenata koji mogu imati utjecaj na izgled stranice
Sjedište weba tijela državne uprave	0% prolaznosti - pronađeno 13 grešaka (5 kritičnih) prevelika stranica korišteno previše vanjskih resursa korišten je javascript detektiran pop-up prozor koji na malom ekranu može izazvati nečitljivost i konfuziju na nekim slikama nedostaju atributi visine i širine zbog čega neki preglednici moraju presložiti stranicu nakon što je učitana korišten nevažeći certifikat.

### 11.10. Ugrađene pristupačne opcije na pokretnim uređajima i računalu

Uređaji s operacijskim sustavom iOS i Android, kao i računala s operacijskim sustavom Windows imaju ugrađene pomoćne značajke koje omogućuju osobama s invaliditetom koristiti funkcionalnosti uređaja kao asistivnih pomagala. Kako bi se ustanovilo u kolikoj mjeri je to ostvarivo i koliko doista ugrađene opcije pristupačnosti mogu koristiti korisnicima sa složenim komunikacijskim potrebama i sa hrvatskog govornog područja, provedeno je testiranje tih opcija na uređajima prikazanim u Tablici 3.6.

**Tablica 3.6.** Pokretni uređaji na kojima su testirane opcije pristupačnosti

Pokretni uređaj	Tip uređaja	Verzija OS
tablet	Samsung Galaxy Tab 2	Android 4.2.2
	Apple Ipad Air	iOS 7.1.1
pametni telefon	Samsung Galaxy Express	Android 4.1.2
	Apple Iphone 4S	iOS7.1.1

### 11.10.1. Pristupačne opcije na uređajima s operacijskim sustavom iOS

*Pristupačne opcije za slabovidne i slijepu osobu:*

- Čitač zaslona VoiceOver djeluje kao posrednik između korisničkog sučelja aplikacije i korisnikovog dodira pružajući zvučne opise elemenata i radnje u primjeni.
  - Aktivira se trostrukim pritiskom na „home“ tipku na iOS uređajima te se sadržaj zaslona interpretira u obliku glasovne poruke: od razine baterije do identifikacije pozivatelja na mobilnom uređaju.
  - Moguća je i podesivost glasnoće zvuka.
  - Aktivacija govornog opisa moguća je i dodiranjem zaslona uređaja prstom. Jednim dodiranjem na izgovorenu aplikaciju pokreće se izgovaranje opisa te aplikacije, a dvostrukim dodiranjem aktivira aplikaciju.
  - Izgovara svako slovo ili znak koji korisnik dodirne na zaslonu unutar email aplikacije, aplikacije za pisanje poruka, izrade bilješki i sl.
  - Omogućuje čitanje i izgovaranje sadržaja emaila, poruka, web stranica i knjiga.
  - Čak i kada je opcija VoiceOver isključena, iOS uređaj može naglas izgovarati odabrani tekst povlačenjem dva prsta po zaslonu odozgo prema dolje na stranici ili aplikaciji koja je trenutno otvorena. Implementirana je i mogućnost podesivosti brzine govora i prilagodba dijalekata u određenim jezicima.
- Siri je ugrađeni „inteligentni pomoćnik“ koji odgovara na pitanja i zahtjeve korisnika. Siri može slati poruke, uspostavljati telefonske pozive, uključivati/isključivati opcije za prilagodbu pristupačnosti. Podržava zapisivanje diktata i prevođenje istog na engleski jezik.
- Povećanje (*Zoom*) je ugrađeno povećalo koje omogućava povećanje sadržaja u novom prozoru dok se izvorni sadržaj zadržava u stvarnoj veličini. Povećanje se može prilagoditi od 100% do 1500%, po želji korisnika, te radi na svim dostupnim aplikacijama na iOS operacijskom sustavu.

- Prilagodba fonta (*Font adjustment*) – prilikom aktivacije mogućnosti “Larger Dynamic Type” tekst unutar aplikacija poput Kontakti, Mail, Poruke, Glazba, Napomene i Postavke, pa čak i nekih aplikacija trećih strana, pretvara se u povećani tekst, lakši za čitanje.
- Invertor boja i sivi tonovi (*Invert colors and grayscale*) – ukoliko veći kontrast ili nedostatak boja pomaže korisniku da bolje vidi sadržaj zaslona, iOS omogućuje zamjenu boja ili omogućuje sive tonove na zaslonu. Filter se nakon postavljanja primjenjuje na cijeli operacijski sustav, čak i na video ili slike.

*Pristupačne opcije za korisnike s poteškoćama sluha:*

- LED svjetlo za alarme – ukoliko korisnik ne može čuti zvukove koji obavještavaju o dolaznim pozivima ili druga upozorenja, iOS uređaj se može prilagoditi da bljeska svojim LED svjetlom na poledini. Ovu opciju je moguće aktivirati samo ako uređaj ima bljeskalicu.
- Mono zvuk i balans – Opcija Mono zvuk kombinira zvuk lijevog i desnog stereokanala u monosignal koji se reproducira kroz oba kanala. Moguće je prilagoditi balans monosignala u cilju dobijanja glasnijeg zvuka lijevog ili desnog kanala. Ova opcija se odnosi na *handsfree* uređaje i slušalice.
- FaceTime je aplikacija za video pozive pomoću kojih korisnik može komunicirati glasovnim ili znakovnim jezikom. Na zaslonu se prikazuju lica korisnika koji sudjeluju u pozivu, koristeći prednje kamere mobilnih ili tablet uređaja.

*Pristupačne opcije za korisnike sa fizičkim i motoričkim poteškoćama:*

- Vođeni pristup (*Assistive touch*) omogućuje prilagodbu zaslona s višestrukim dodirima uređaja na specifične fizičke potrebe. Ukoliko korisnik ima poteškoća s nekim gestama može ih učiniti pristupačnim tako da tu gestu zamijeni jednostavnim dodirima prsta na zaslon uređaja ili može stvoriti vlastitu gestu koja će zamijeniti postojeću. Geste poput rotacije i mahanja su dostupni i kada je iOS uređaj montiran na invalidska kolica.
- Kontrola prekidača (*Switch Control*) omogućuje upravljanje pametnim telefonom (iPhone) koristeći jedan ili više prekidača (vanjskih uređaja). Potrebno je odabrati metodu za postupke poput odabira, dodirivanja, povlačenja, tipkanja ili crtanja rukom. Osnovna tehnika je da korisnik koristi prekidač za odabir stavke ili mjesta na zaslonu i zatim pomoću istog (ili različitog) prekidača odabere postupak za izvođenje na toj stavci ili mjestu.
- Predvidljivo tipkanje (*Predictive Text*) je mogućnost koja prilikom tipkanja operacijski sustav nudi iOS predložene riječi i fraze za nadopunjavanje rečenica na određenom jeziku što ubrzava proces unosa teksta.

### 11.10.2. Pristupačne opcije na uređajima s operacijskim sustavom Android

#### *Pristupačne opcije za slabovidne i slijepo osobe:*

- TalkBack je instalirana usluga za čitanje zaslona koju pruža Google za slabovidne i slijepo korisnike. Upotrebljava izgovorene povratne informacije za opis radnji, primjerice, otvaranje aplikacija i događaja kao što su obavijesti. Koristi vibraciju i zvučne signale kako bi korisniku dao do znanja što se nalazi na ekranu i što dodiruje. Ako je uključena opcija *Istraživanje dodirrom (Touch exploration)*, uređaj čita sve preko čega korisnik prijeđe prstima. TalkBack može izgovarati ID pozivatelja, čitati nazive tipki koje korisnik pritisne na tipkovnici te čitati tekst poput vremenske prognoze i obavijesti, čak i kada je zaslon isključen. Moguće je podesiti glasnoću govora i visinu glasa, uključiti i isključiti vibraciju te kod uređaja koji imaju senzor blizine, uključiti utišavanje govora ako se korisnik približi uređaju. Postoji opcija kojom se omogućava kontinuirano čitanje s ekrana ako korisnik protrese uređaj.
- Opcija pretvaranja teksta u govor (*Text-to-speech*) po predefiniranim postavkama koristi Google-ov sintetizator govora, ali je s Play Store-a moguće preuzeti i druge sintetizatore trećih strana. Moguće je podesiti jezik za izgovaranje i brzinu govora.
- Pokreti za povećavanje (*Magnification gestures*) su značajka pristupačnosti pomoću koje se privremeno povećava prikaz na zaslonu ili rabi način povećanja za jednostavno zumiranje i pomicanje zaslona. Kada je ova značajka uključena, može se povećavati i smanjivati zumiranje tako da se triput dodirne zaslon. Trostruko dodirivanje za povećavanje može se upotrijebiti svugdje osim za tipkovnicu i navigacijske gumbе. Opcija je dostupna samo na tabletu koji je korišten u svrhu testiranja, ali ne i na korištenom pametnom telefonu.
- Veličina fonta (*Font size*) je opcija kojom se može promijeniti veličina fonta na svim aplikacijama koje dolaze s uređajem. Veličina se ne mijenja na svim aplikacijama iz *Play Store*-a i na početnom ekranu.
- Negativ (*Negative colors*) je opcija koja zamjenjuje boje s njihovim negativom kako bi slabovidnim osobama omogućio lakše čitanje teksta na ekranu.
- *BrailleBack* je dodatna usluga pristupačnosti koja slijepim korisnicima omogućuje uporabu *Brailleovih* uređaja. U kombinaciji s aplikacijom *TalkBack* povratne se informacije dobivaju na *Brailleovom* pismu i govorom. Pomoću te aplikacije može se povezati na podržani *Brailleov* uređaj preko *Bluetootha*. Sadržaj zaslona prikazuje se na uređaju, a tipke na zaslonu omogućuju kretanje uređajem i interakciju s njime.

#### *Pristupačne opcije za osobe s poteškoćama sluha:*

- Korekcija zvuka (*Sound balance*) je opcija kojom se postiže glasniji zvuk u lijevom ili desnom kanalu pri korištenju slušalica.

- Mono zvuk (*Mono sound*) je opcija kojom se mijenja zvuk iz stereo u mono pri korištenju jedne slušalice.

### 11.10.3. Pristupačnost na operacijskom sustavu Windows 8.1

Dio upravljačke ploče Ease of Access Center na sustavu Windows upravlja postavkama pristupačnosti. Na njemu se za korisnike s određenim poteškoćama mogu izvesti određene prilagodbe prikaza tijekom rada s računalom.

#### *Opcije za slabovidne i slijepe osobe:*

- Povećalo (*Magnifier*) je alat koji uvećava dio ili cijeli zaslon, kako bi korisnik mogao bolje vidjeti tekst i slike. Može se koristiti pomoću miša ili dodirivanjem zaslona na dodir. Postoji nekoliko načina rada povećala:
  - full-screen – poveća se cijeli zaslon te se može pregledavati dio po dio,
  - lens (leća) – miš postaje povećalo i uvećava dio zaslona na koji ga se postavi
  - docked – dio zaslona nad kojim se nalazi miš vidimo prikazuje se u uvećanom prozoru koji se može smjestiti bilo gdje na radnoj površini.
- Virtualna tipkovnica (*On-screen Keyboard*) je opcija koja prikazuje tipkovnicu na zaslonu. Možemo se koristiti pomoću miša ili dodirivanjem zaslona na dodir. Dostupna je i opcija predviđanja teksta koja predlaže riječi dok korisnik piše s navedenom tipkovnicom, čime mu se ubrzava i olakšava proces unošenja teksta.
- Pripovjedač (*Narrator*) je alat koji čita tekst i opisuje što se nalazi na ekranu. Vrlo se lako uključuje i isključuje (*Windows + Enter*) te nudi opcije poput mijenjanja tona, brzine i visine glasa, čitanja riječi koje se unose te stišavanja ostalih aplikacija dok je uključen. Pomoću opcije se može koristiti računalo bez zaslona. Opcija je podržana samo za engleski jezik.
- Prepoznavanje glasa (*Speech Recognition*) čini korištenje miša i tipkovnice opcionalnim te omogućava upravljanje računala glasom.
- Promjena veličine teksta (*Change text size*) je opcija koja povećava tekst i objekte bez gubitka kvalitete da bi bili uočljiviji. Opcija je podržana samo za engleski jezik.

#### *Opcije za osobe s poteškoćama sluha:*

- Vizualne notifikacije (*Visual notifications*) zamjenjuju sistemske zvukove sa vizualnim efektima poput npr. treperenja ekrana. Također je moguće aktivirati titlove za pojedine zvukove, tj. da se na ekranu ispiše što pojedini zvuk znači.



#### 11.10.4. Analiza opcija pristupačnosti na primjeru zadanog sjedišta weba

Ugrađene opcije pristupačnost testirane su za projektno sjedište web za korisnike potpomognute komunikacije<sup>57</sup> koje ima relativno loš rezultat testiranja alatom mobileOK Checker. Cilj testiranja je bio ustanoviti koliko opcije pristupačnost mogu poboljšati prilagođenost ovog sjedišta weba osobama sa složenim komunikacijskim potrebama koje ga pretražuju na svojim pokretnim uređajima (tabletu i pametnom telefonu).

#### Uređaji s operacijskim sustavom iOS

- **Pristupačne opcije za slabovidne:**
  - **Voice over** - funkcionira na svim elementima stranice no izgovor je nerazumljiv jer nema podršku za hrvatski jezik. Na engleskom jeziku izgovara tekst svakog paragrafa koji se odabere.
  - **Speak screen** - izgovoreni tekst je u potpunosti nerazumljiv jer nema mogućnost izgovora hrvatskog jezika.
  - **Zoom** - podržanost 100%. Stranica se u potpunosti prilagođava korisnikovim potrebama.
  - **Prilagodba fonta** - ne funkcionira na stranici. Ova mogućnost funkcionira samo na aplikacijama, ne na web stranicama unutar internet preglednika.
  - **Invertor boja** - boje na stranici se u potpunosti invertiraju, uključujući boje na slikama koje su sastavni dio sadržaja stranice (Slika 3.3.).



**Slika 3.3.** Efekt invertiranja boja primijenjen na web stranici projekta ICT-AAC

---

<sup>57</sup> ICT-AAC, [www.ict-aac.hr](http://www.ict-aac.hr)

- **Opcije za korisnike sa slušnim poteškoćama:**

- Nema pristupačnih mogućnosti koje podržavaju zadanu web stranicu
- Napomena: Ove mogućnosti funkcioniraju na razini operacijskog sustava iOS, tj. funkcioniraju samo u određenim aplikacijama razvijenim za taj sustav. Funkcionalnosti su testirane za sjedište weba ICT-AAC u pregledniku Safari, no Safari nema integrirane mogućnosti za korisnike sa slušnim poteškoćama (npr. nema mogućnost upravljanja LED svjetlom na poledini uređaja).

- **Pristupačne opcije za korisnike sa fizičkim i motoričkim poteškoćama:**

- Nema pristupačnih mogućnosti koje podržavaju web stranicu
- Ove opcije funkcioniraju na razini operacijskog sustava mobilnog i tablet uređaja te se ne mogu pokrenuti kod pregledavanja web stranica u pregledniku

### **Uređaji s operacijskim sustavom Android**

- **Pristupačne opcije za slabovidne:**

- TalkBack i sintetizator govora - funkcioniraju na svim elementima stranice, ali izgovara hrvatski tekst na engleskom jeziku zbog čega je većina toga nerazumljiva.
- Pokreti za povećanje - funkcioniraju na svim dijelovima operacijskog sustava i na web stranicama.
- Veličina fonta - mijenjanje veličine fonta u postavkama sustava ne utječe na izgleda web stranice.
- Negativ - radi kako treba, sve boje su zamijenjene svojim negativima.
- BrailleBack - za testiranje ove opcije bi bio potreban dodatan uređaj koji tekst pretvara u Braille--- ovo pismo, no s obzirom da on radi u suradnji s TalkBack--om, a TalkBack radi ispravno, možemo se pretpostaviti da bi i BrailleBack isto tako radio ispravno.

Testiranjem ugrađenih opcija pristupačnosti na pokretnim uređajima (tableti i pametni telefoni) može se zaključiti kako vrlo malo opcija za poboljšanje pristupačnosti funkcionira za pregledavanje web stranice u pregledniku koja nije dizajnirana u skladu s preporukama WAI. Jedine opcije koje se mogu primijeniti su zumiranje, odnosno pokreti za povećanje i invertor boja. Sintetizatori govora *Voice over* i *TalkBack* čitaju tekst, ali na engleskom i nerazumljivo, dok opcije za prilagodbu fonta ne rade na web stranicama. Rješenje je dakle u implementaciji web dizajna koji ima ugrađene elemente pristupačnosti prema definiranim smjernicama.

### 11.11. Zaključak

Danas postoji veći broj projekata, inicijativa, partnerstva u okviru kojih su razvijena ICT rješenja koja pokušavaju poboljšati kvalitetu života i socijalnu uključenost osoba sa složenim komunikacijskim potrebama, odnosno osoba s invaliditetom i osoba starije dobe. Također postoji veliki broj projekata i inicijativa u području gerontotehnologije i asistivne tehnologije čije su aktivnosti usmjerene prema definiranju načela, preporuka i smjernica čijom se implementacijom mogu realizirati pristupačna rješenja za navedene skupine korisnika. Neka istraživanja ukazuju da se pri rehabilitaciji osoba oboljelih od neurodegenerativnih bolesti, poput Alzheimerove bolesti i demencije mogu postići izvrsni rezultati primjenom dobro dizajniranih i osmišljenih ICT rješenja.

Nove generacije pokretnih uređaja zbog svojih tehnoloških mogućnost pružaju veliki potencijal korisnicima kao alati za svakodnevnu podršku, ali i osobama koje skrbe o korisnicima s invaliditetom i osobama starije dobi za kontinuirani nadzor zdravstvenog stanja. No u isto vrijeme ti uređaji često predstavljaju barijere osobama s poteškoćama vida, sluga, kognitivnim i motoričkim poteškoćama.

Uređaji novih generacija imaju ugrađene opcije pristupačnosti koje bi trebale omogućiti osobama s određenim fizičkim poteškoćama da svoje uređaje koriste kao asistivne tehnologije.

Istraživanje koje je provedeno s ciljem analize usluga weba kao najraširenijeg ICT rješenja današnjice, za primjer najposjećenijih stranica hrvatskog kataloga sjedišta weba [www.hr](http://www.hr) pokazuje da se u dizajnu još uvijek ne vodi dovoljno računa o pristupačnosti i potrebama specifičnih kategorija korisnika. Na primjer, samo dva od četrnaest analiziranih news portala imaju potpuno pristupačan dizajn. Također, testirane su ugrađene opcije pristupačnosti na pokretnim uređajima s operacijskim sustavima iOS i Android te računalu s operacijskim sustavom Windows 8 za primjer sjedišta koje nema pristupačni dizajn s ciljem evaluacije do koje mjere opcije uređaja mogu poboljšati pristupačnost. Analiza je pokazala da se za hrvatske korisnike svega može primijeniti nekoliko ugrađenih opcija funkcionalnost čime se ne postiže gotovo nikakvo poboljšanje pristupačnosti. Zaključak je da je dakle najveća odgovornost na razvoju pristupačnog web dizajna ili na razvoju novih usluga koje će moći interpretirati sadržaj pojedinog web sjedišta i automatski napraviti prilagodbu u skladu s potrebama pojedinih kategorija korisnika te na taj način premostiti navedeni nedostatak pristupačnosti dizajna.

### 11.12. Literatura

[1] Katalog znanja o potpomognutoj komunikaciji, ICT sustavi za osobe sa složenim komunikacijskim potrebama, <http://www.ict-aac.hr/index.php/hr/katalog-znanja>

[2] Transgenerational Design Matters, *The demographics of aging*, <http://transgenerational.org/aging/demographics.htm>

- [3] Patsoule Evelina, Panayiotis Koutsabasis, Redesigning websites for older adults: a case study, *Behaviour & Information Technology*, Vol. 33, Iss. 6, 2014
- [4] *Web Accessibility for Older Users: A Literature Review*, <http://www.w3.org/TR/wai-age-literature/#arfl>
- [5] European Innovation Partnership on Active and Healthy Ageing, action plan D4 on 'Innovation for Age-friendly buildings, cities & environments', [http://ec.europa.eu/research/innovation-union/pdf/active-healthy-ageing/d4\\_action\\_plan.pdf](http://ec.europa.eu/research/innovation-union/pdf/active-healthy-ageing/d4_action_plan.pdf)
- [6] Redish, J. and Chisnell, D. Designing Web Sites for Older Adults: A Review of Recent Literature. Prepared for AARP, December 2004, [http://assets.aarp.org/www.aarp.org/\\_articles/research/oww/AARP-LitReview2004.pdf](http://assets.aarp.org/www.aarp.org/_articles/research/oww/AARP-LitReview2004.pdf)
- [7] Kowtko, M., "Using assistive technologies to improve lives of older adults and people with disabilities," Systems, Applications and Technology Conference (LISAT), 2012 IEEE Long Island, vol., no., pp.1,6, 4-4 May 2012
- [8] Designing Accessible Web Forms, 2014., *Designing Accessible Web Forms*, <http://www.afb.org/info/accessibility/creating-accessible-websites/accessible-forms/235>, 27.10.2014.
- [9] Improving web accessibility for People with Disabilities, 2014., *Improving web accessibility for People with Disabilities*, <http://www.and.org.au/pages/improving-web-accessibility-for-people-with-disabilities.html>, 27.10.2014.
- [10] National Institute on Aging, *Making Your Website Senior Friendly*, <http://www.nia.nih.gov/health/publication/making-your-website-senior-friendly>
- [11] *Developing Websites for Older People: How Web Content Accessibility Guidelines (WCAG) 2.0 Applies*, <http://www.w3.org/WAI/older-users/developing.html>
- [12] José-Manuel Díaz-Bossini, Lourdes Moreno, Accessibility to Mobile Interfaces for Older People, *Procedia Computer Science*, Volume 27, 2014, Pages 57-66, ISSN 1877-0509
- [13] *Web Accessibility and Older People: Meeting the Needs of Ageing Web Users*, <http://www.w3.org/WAI/older-users/>

## 12. Kalkulator za procjenu rizika povrede privatnosti korisnika

### 12.1. Uvod

U kontekstu privatnosti korisnika u internetskim uslugama, značajan problem predstavlja činjenica da korisnici nisu svjesni rizika i potencijalnih posljedica po privatnost koje može prouzročiti nepažljivo odavanje privatnih podataka. U radu objavljenom na konferenciji SoftCOM 2014 [1] i prošlom izvještaju [2] izneseni su opis i model kalkulatora za procjenu rizika povrede privatnosti korisnika te njegova evaluacija. Kalkulator je zasnovan na umjetnim neuronskim mrežama koje procjenjuju rizik povrede privatnosti korisnika, a njegov glavni cilj pokušati je podići svijest o opasnostima među korisnicima internetskih usluga. U ovom izvještaju izložen je osvrt na mogućnosti aktualne razvojne verzije kalkulatora uz korisničke upute o tome kako ga koristiti te pojašnjenje izračunatih vrijednosti.

Kalkulator za procjenu rizika povrede privatnosti za ulazne vrijednosti uzima korisničke parametre (njih 9, vidljivi na Slici 4.1.) koje zahtijevaju pojedine aplikacije i usluge. Izlazne vrijednosti su procjena rizika praćena opisom nekoliko scenarija iz stvarnog života. Scenariji su realizirani kao kratki stripovi koji su razvijeni pomoću web-aplikacije za izradu stripova Pixton [3]. Kalkulator je implementiran u obliku web-aplikacije i krajnji korisnici moći će mu jednostavno pristupiti putem svojih preglednika weba. Trenutna verzija kalkulatora u fazi razvoja dostupna je na [4].

Svaki pojedini korisnički parametar uz sebe nosi i određene rizike povrede privatnosti ukoliko bude ukraden i zloupotrebljen. Nadalje, kombiniranje više parametara zajedno agregira rizike. Svakom uzorku ulaznih parametara na izlazu se dodjeljuje vrijednost koja predstavlja procjenu rizika. Karakteristične izlazne vrijednosti su 0.33, 0.66 i 0.99, što predstavlja gornju granicu niske, srednje i visoke razine rizika povrede privatnosti. Tumačenje značenja tih izlaznih vrijednosti je sljedeće:

- niska razina rizika (0.33 i niže) ne predstavlja izravnu opasnost za korisnika; napadač može pokušati iskoristiti privatne podatke za prijevare korisnika ili treće osobe s neizvjesnim ishodom.
- srednja razina rizika (0.34-0.66) daje napadaču mogućnost iskorištavanja privatnih korisničkih podataka u pokušaju prijevare korisnika ili treće osobe, uz višu razinu uspjeha; ciljano sudjelovanje korisnika može biti potrebno.
- visoka razina rizika (0.67-0.99) ukazuje na to da napadač može napraviti znatnu štetu korisniku ili trećim osobama, bez potrebe za daljnjim obmanjivanjem korisnika ili zahtijevom za njegovim dodatnim sudjelovanjem.

Kako bi se korisnicima dao bolji uvid u potencijalne opasnosti, uz svaku brojčanu procjenu rizika povrede privatnosti dolazi i opis (u obliku stripa) nekoliko scenarija iz svakodnevnog života do kojih može doći zbog neopreznog rukovanja privatnim podacima.

## 12.2. Upute za korištenje

Kalkulator za procjenu rizika povrede privatnosti jednostavan je za uporabu. Korisnik u pregledniku weba otvara stranicu s kalkulatorom. Odabire jedan ili više od ukupno devet dostupnih korisničkih parametara, ovisno o zahtjevima internetske usluge za koju želi procijeniti rizik potencijalne povrede privatnosti (Slika 4.1.):

- e-mail adresa, ime i prezime, spol, datum rođenja, država, broj mobitela, adresa, javni profil društvene mreže, podaci kreditne kartice;



**Slika 4.1.** Početna stranica kalkulatora rizika

Nakon odabira korisničkih parametara, kalkulator procjenjuje rizik povrede privatnosti i njegovu razinu (visoka (primjer na Slika 4.2.), srednja (primjer na Slika 4.3.) ili niska (primjer na Slika 4.4.)), te ako je dostupan u obliku kratkog stripa daje scenarij koji koristi te parametre i može prouzročiti povredu privatnosti. Ako odabrana kombinacija korisničkih

parametara može biti zlopotrebljena u više različitih scenarija, daje se pregled svih uz pripadajuće stripove (primjer na Slika 4.3.).



**Slika 4.2.** Primjer scenarija uz visoku razinu rizika (ulazni parametar „kreditna kartica“)



Slika 4.3. Primjer scenarija uz srednju razinu rizika (ulazni parametar „e-mail adresa“)





**Slika 4.4.** Primjer scenarija uz nisku razinu rizika (ulazni parametar „datum rođenja“)

Klikom miša na sažetu verziju stripa otvara se verzija stripa preko cijelog ekrana za lakše pregledavanje. Za korištenje kalkulatora korisnik osim web-pretraživača nove generacije (Internet Explorer, Mozilla Firefox, Google Chrome) s podrškom za Flash ne mora imati na raspolaganju nikakvu drugu programsku potporu.

### 12.3. Popis stripova

Trenutna baza stripova koji objašnjavaju scenarije iz svakodnevnog života a mogu dovesti do povrede privatnosti korisnika sadrži pet stripova:

- nigerijska prijevara (*Nigerian scam*) (Slika 4.5.);
- *phishing* (Slika 4.6.);
- instalacija zlonamjernog softvera (Slika 4.7.);
- *on-line* druženje (Slika 4.8.);
- *on-line* kupovina (Slika 4.9.);

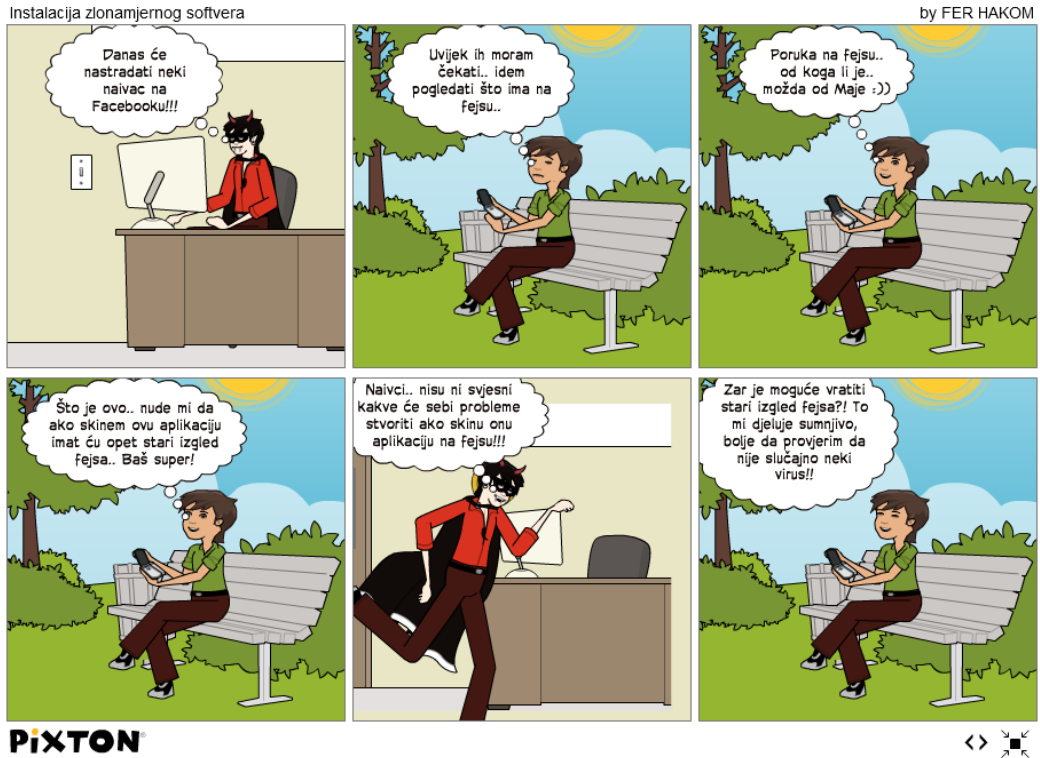
Sukladno izdavanju novih verzija kalkulatora, plan je postupno proširivati bazu stripova.



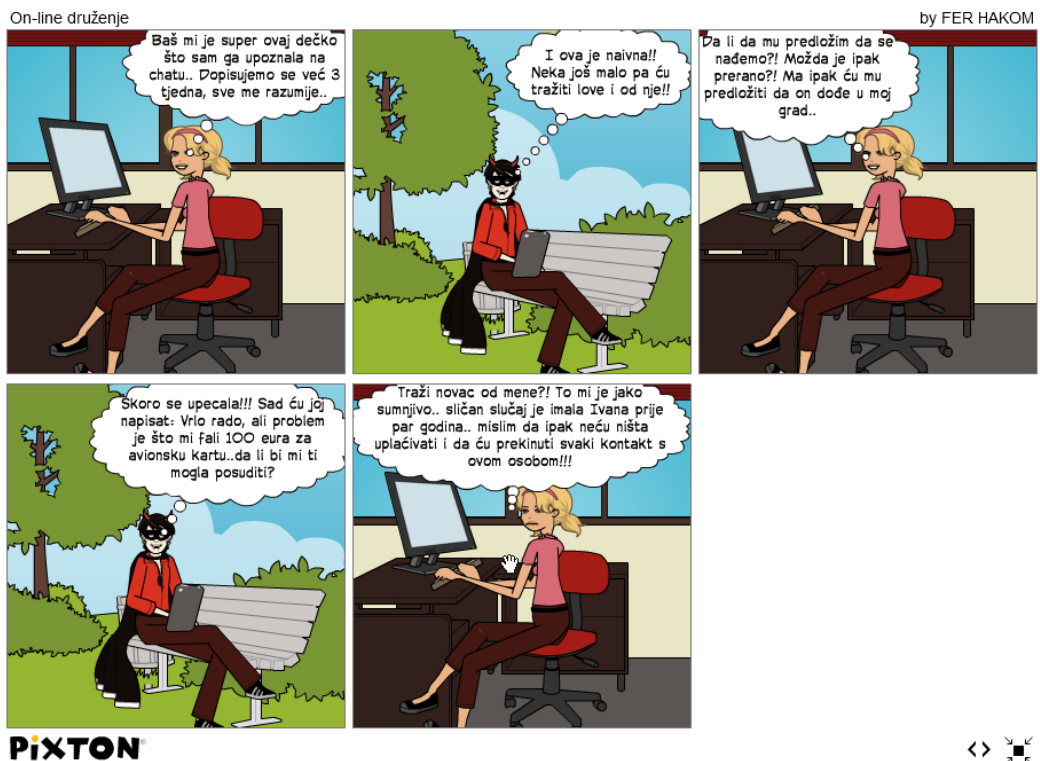
Slika 4.5. Strip „Nigerijska prijevara“



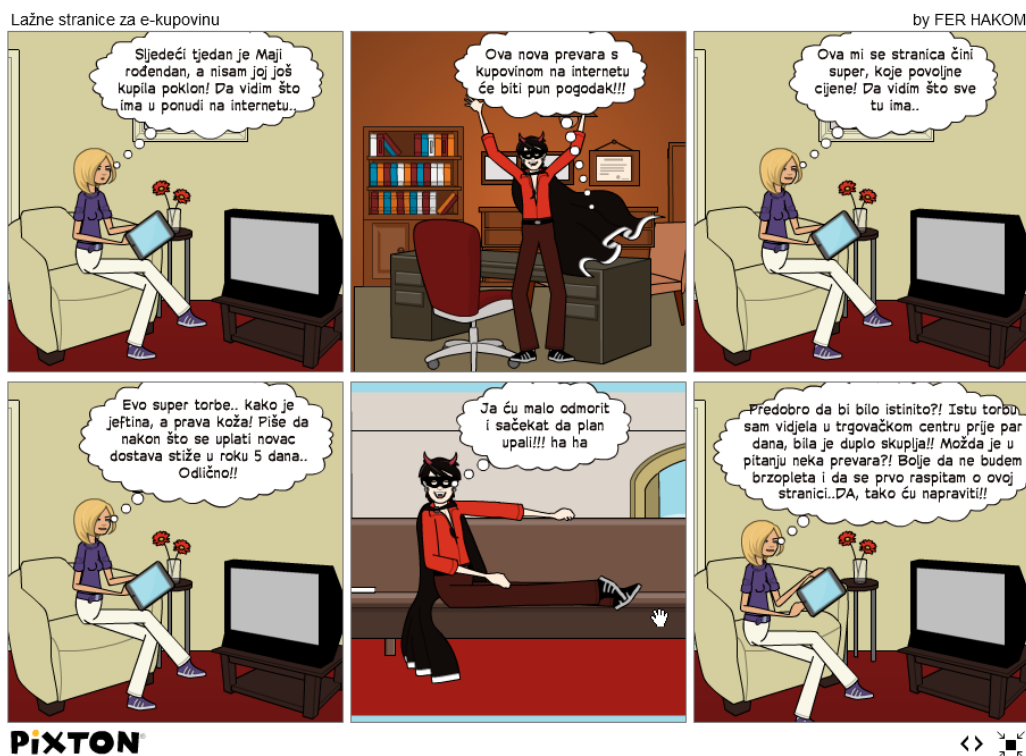
Slika 4.6. Strip „Phishing“



Slika 4.7. Strip „Instalacija zlonamjernog softvera“



Slika 4.8. Strip „On-line druženje“



Slika 4.9. Strip „Lažne stranice za e-kupovinu“

## 12.4. Literatura

[1] M. Vuković, D. Katušić, P. Skočir, D. Jevtić, L. Delonga, D. Trutin: „User Privacy Risk Calculator“, u zborniku radova konferencije *22nd International Conference on Software, Telecommunications and Computer Networks (SoftCOM 2014)*, Split, Hrvatska, 2014.

[2] Evaluacija kalkulatora za procjenu rizika povrede privatnosti korisnika, izvješće „Regulatorni aspekti budućih mreža, privatnost i uključivost usluga i njihova kvaliteta“, projekt „Pogled u budućnost 2020“, treći kvartal 2014.

[3] Pixton, <http://www.pixton.com/>

[4] Razvojna verzija kalkulatora za procjenu rizika povrede privatnosti korisnika, <http://hakom.tel.fer.hr/index.php>